P-793H v2

G.SHDSL.bis Bonded Broadband Gateway

Support Notes

Version 3.70
02/2010

FAQ 4
ZyNOS FAQ 4
1. What is ZyNOS? 4
2. How do I access the P-793H v2 SMT menu? 4
3. How do I upload the ZyNOS firmware code via console? 4
4. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN? 4
6. How do I restore P-793H v2 configurations by using TFTP client program via LAN? 5
7. What should I do if I forget the system password? 5
8. How to use the Reset button? 5
9. What is SUA? When should I use SUA? 6
10. What is the difference between SUA and Full Feature NAT? 6
11. Is it possible to access a server running behind SUA from the outside Internet? If possible, how? 7
12. When do I need to select Full Feature NAT? 7
13. What IP/Port mapping does Multi-NAT support? 7
14. How many network users can the SUA/NAT support? 8
15. What are Device filters and Protocol filters? 9
16. How can I protect against IP spoofing attacks? 9
Product FAQ 11
1. What is SHDSL, SHDSL.bis? 11
2. How can I manage P-793H v2? 11
3. What is the default password for Web Configurator? 11
4. What's the difference between 'Common User Account' and 'Administrator Account'? 11
5. How do I know the P-793H v2's WAN IP address assigned by the ISP? 11
6. What do I need before using the SHDSL? 12
7. What should I do when the power (PWR) LED is off? 12
8. How to debug while DSL LED is off? 12
9. How do I verify my PC's IP address assigned by the P-793H v2? .. 12
10. What is Traffic Shaping? 12
11. What do the parameters (PCR, SCR, MBS) mean? 12
12. What do ATM QoS Types (CBR, UBR, VBR-nRT, VBR-RT) mean? 13
13. Why do we perform traffic shaping in the P-793H v2? 13
14. The P-793H v2 supports Bridge and Router mode, what's the difference between them? 14
15. How do I know I am using PPPoE? 14
16. Why does my provider use PPPoE? 14
17. What is DDNS? 14
18. When do I need DDNS service? 15

All contents copyright © 2010 ZyXEL Communications Corporation.

19. What is DDNS wildcard? Does the P-793H v2support DDNS wildcard? 15
20. Can the P-793H v2's SUA handle IPSec packets sent by the IPSec gateway? 15
21. How do I setup my P-793H v2 for routing IPSec packets over SUA? 15
22. What is VLAN? 16
23. 802.1Q/1P 16
24. What is Traffic Redirect ? 17
25. What is Dial Backup? 17
DSL FAQ 17
1. How does DSL compare to Cable modems? 17
2. How do I know the DSL line is up? 18
3. How does the P-793H v2 work on a noisy DSL? 18
4. Does the VC-based multiplexing perform better than the LLC-based multiplexing? 18
5. How do I know the details of my DSL line statistics? 18
6. What are the signaling pins of the DSL connector? 19
7. What is triple play? 19
Firewall FAQ 20
General 20
Configuration 23
Log and Alert 26
IPSec FAQ 28
VPN Overview 28
P-793H v2 VPN 32
Application Notes 38
General Application Notes 38
1. Internet Access Using P-793H v2 under Bridge mode 38
2. Internet Access Using P-793H v2 under Routing mode 40
3. Internet Access scenarios 42
4. Back to back scenarios 43
5. What is the checklist for making a 1-1 Back-to-Back connection over P-793H v2? 44
6. What is the checklist for making a 1-2 Back-to-Back connection over P-793H v2? 45
7. Setup the P-793H v2 as a DHCP Relay. 45
8. SUA Notes 46
9. Using Full Feature NAT 55
10. Using the Dynamic DNS (DDNS) 63
11. Network Management Using SNMP 65
12. Using syslog 68
13. Using IP Alias 68
14. Using IP Policy Routing 71

All contents copyright © 2010 ZyXEL Communications Corporation.

15. Using Call Scheduling 73
16. Using IP Multicast 75
17. Using Bandwidth Management 76
18. How to configure packet filter on P-793H v2? 79
19. How could I configure triple play on P-793H v2? 79
20. How to setup traffic redirect in P-793H v2? 80
21. How to deal with Triangle Route and Traffic redirect? 82
22. How to setup Dial Backup? 85
IPSEC VPN Application Notes 86
1. How to use P-793H v2 to build VPN Tunnel with another VPN Gateway/ Software? 86
2. How to build a VPN between Secure Gateway with Dynamic WAN IP Address? 92
3. Configure NAT for internal servers 94
4. VPN Routing between Branch Office through Headquarter 95
Support Tool 99
1. LAN/WAN Packet Trace 99
2. Firmware/Configurations Uploading and Downloading using TFTP 103
3. Using FTP to Upload the Firmware and Configuration Files 106
CI Command Reference 109
Reference 110
1. PPP Numbers 110
2. Port Numbers 122
3. Protocol Numbers 126

All contents copyright © 2010 ZyXEL Communications Corporation.

FAQ

ZyNOS FAQ

1. What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all P-793H v2 routers that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites as they become available.

2. How do I access the P-793H v2 SMT menu?

The SMT interface is a menu driven interface, which can be accessed via a RS232 console or a Telnet connection. To access the P-793H v2 via SMT console port, a computer equipped with communication software such as HyperTerminal must be configured to the following parameters.

- VT100 terminal emulation
- 9600bps baud rate
- N81 data format (No Parity, 8 data bits, 1 stop bit)

The default console port baud rate is 9600bps, you can change it to 115200bps in Menu 24.2.2 to speed up access of the SMT.

3. How do I upload the ZyNOS firmware code via console?

The procedure for uploading via console is as follows.

(1) Enter debug mode when powering on the P-793H v2 using a terminal emulator
(2) Enter 'ATUR' to start the uploading
(3) Use X-modem protocol to transfer the ZyNOS code
(4) Enter 'ATGO' to restart the P-793H v2

4. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN?

The P-793H v2 allows you to transfer the firmware from/to P-793H v2 by using TFTP program via LAN. The procedure for uploading via TFTP is as follows.

All contents copyright © 2010 ZyXEL Communications Corporation.

(1) Use the TELNET client program in your PC to login to your P-793H v2, and use Menu 24.8 to enter CI command 'sys stdio 0' to disable console idle timeout
(2) To upgrade firmware, use TFTP client program to put firmware in file 'ras' in the P-793H v2. After data transfer is finished, the P-793H v2 will program the upgraded firmware into FLASH ROM and reboot itself.
(3) To backup your firmware, use the TFTP client program to get file 'ras' from the P-793H v2.

5. How do I upload ROMFILE via console port?

In some situations, you may need to upload the ROMFILE, such as losing the system password, or the need of resetting SMT to factory default.

The procedure for uploading via the console port is as follows.

(1) Enter debug mode when powering on the P-793H v2 using a terminal emulator
(2) Enter 'ATLC' to start the uploading
(3) Use X-modem protocol to transfer ROMFILE
(4) Enter 'ATGO' to restart the P-793H v2

6. How do I restore P-793H v2 configurations by using TFTP client program via LAN?

(1) Use the TELNET client program in your PC to login to your P-793H v2.
(2) Enter CI command **'sys stdio 0'** disable Stdio idle timeout
(3) To backup the P-793H v2 configurations, use TFTP client program to get file **'rom-0'** from the P-793H v2.
(4) To restore the P-793H v2 configurations, use the TFTP client program to put your configuration in file **rom-0** in the P-793H v2.

7. What should I do if I forget the system password?

In case you forget the system password, you can erase the current configuration and restore factory defaults this way:

Use the **RESET button** on the rear panel of P-793H v2 to reset the router. After the router is reset, the LAN IP address will be reset to **'192.168.1.1',** the common user password will be reset to **'user',** the Administrator password will be reset to '**1234'.**

8. How to use the Reset button?

(1) Turn your P-793H v2 on. Make sure the **POWER** led is on (not blinking)

All contents copyright © 2010 ZyXEL Communications Corporation.

(2) Press the **RESET** button for longer than one second and shorter than five seconds and release it. If the **POWER** LED begins to blink, the P-793H v2's wireless auto security function-**OTIST** has been enabled.

(3) Press the **RESET** button for six seconds and release it. If the **POWER** LED begins to blink, the default configuration has been restored and the P-793H v2 restarts.

9. What is SUA? When should I use SUA?

SUA (Single User Account) is a unique feature supported by P-793H v2 router which allows multiple people to access Internet concurrently for the cost of a single user account.

When P-793H v2 acts as SUA receives a packet from a local client destined for the outside Internet, it replaces the source address in the IP packet header with its own address and the source port in the TCP or UDP header with another value chosen out of a local pool. It then recomputes the appropriate header checksums and forwards the packet to the Internet as if it is originated from P-793H v2 using the IP address assigned by ISP. When reply packets from the external Internet are received by P-793H v2, the original IP source address and TCP/UDP source port numbers are written into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to its true destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

10. What is the difference between SUA and Full Feature NAT?

When you edit a remote node in Web Configurator, Advanced Setup, **Network -> Remote Node -> Edit,** there will be three options for you:

- **None**
- **SUA Only**
- **Full Feature**

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules: **Many-to-One** and **Server**. With SUA, 'visible' servers had to be mapped to different ports, since the servers share only one global IP.

The P-793H v2 now has **Full Feature NAT** which supports five types of IP/Port mapping: One to One, Many to One, Many to Many Overload, Many to Many No Overload and Server. You can make special application when you select **Full Feature NAT**. For example: With multiple global IP addresses, multiple severs using the same port (e.g., FTP servers using port 21/20) are allowed on the LAN for outside access.

All contents copyright © 2010 ZyXEL Communications Corporation.

The P-793H v2 supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The P-793H v2 supports 8 sets since there are 8 remote nodes.

By factory default, the NAT is select as **SUA** in Web Configurator, Advanced Setup, **Network -> NAT -> General -> NAT Setup.**

11. Is it possible to access a server running behind SUA from the outside Internet? If possible, how?

Yes, it is possible because P-793H v2 delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured. (You can configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding**).

12. When do I need to select Full Feature NAT?

- Make multiple local servers on the LAN accessible from outside with multiple global IP addresses

With SUA, 'visible' servers had to be mapped to different ports, since the servers share only one global IP. But when you select **Full Feature**, you can make multiple local servers (mapping the same port or not) on the LAN accessible from outside with multiple global IP addresses.

- Support Non-NAT Friendly Applications

Some servers providing Internet applications such as some MIRC servers do not allow users to login using the same IP address. Thus, users on the same network can not login to the same server simultaneously. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user login to the server using a unique global IP address.

13. What IP/Port mapping does Multi-NAT support?

Multi-NAT supports five types of IP/port mapping: One to One, Many to One, Many to Many Overload, Many to Many No Overload and Server. The details of the mapping between ILA and IGA are described as below. Here we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA),

- **One to One**: In One-to-One mode, the P-793H v2 maps one ILA to one IGA.

All contents copyright © 2010 ZyXEL Communications Corporation.

- **Many to One:** In Many-to-One mode, the P-793H v2 maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA is optional in today's P-793H v2 routers).
- **Many to Many Overload:** In Many-to-Many Overload mode, the P-793H v2 maps multiple ILA to shared IGA.
- **Many One-to-One:** In Many One-to-One mode, the P-793H v2 maps each ILA to unique IGA.
- **Server:** In Server mode, the P-793H v2 maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note, if you want to map each server to one unique IGA please use the One-to-One mode.

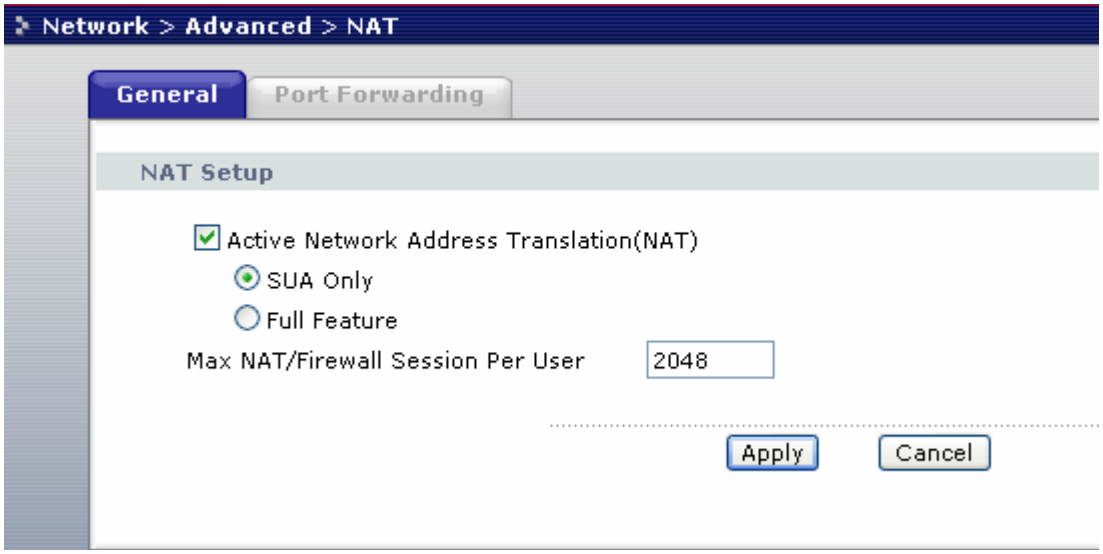
The following table summarizes the five types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 …
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 …
Many One-to-One	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 …
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

14. How many network users can the SUA/NAT support?

The P-793H v2 does not limit the number of the users but the number of the NAT sessions. The P-793H v2 supports 2048 sessions that you can use the **'ip nat session'** command in CLI to see. You can also use '**ip nat hashTable wanif0**' to view the current active NAT sessions. Or you can check it in below WEB Configurator.

All contents copyright © 2010 ZyXEL Communications Corporation.



15. What are Device filters and Protocol filters?

In ZyNOS, the filters have been separated into two groups. One group is called 'device filter group', and the other is called 'protocol filter group'. Generic filters belong to the 'device filter group', TCP/IP and IPX filters belong to the 'protocol filter group'. You can configure the filter rule in SMT.

Note: In ZyNOS, you can not mix different filter groups in the same filter set.

16. How can I protect against IP spoofing attacks?

The P-793H v2's filter sets provide a means to protect against IP spoofing attacks. The basic scheme is as follows:

For the input data filter:

- Deny packets from the outside that claim to be from the inside
- Allow everything that is not spoofing us

Filter rule setup:

- Filter type =TCP/IP Filter Rule
- Active =Yes
- Source IP Addr =a.b.c.d
- Source IP Mask =w.x.y.z
- Action Matched =Drop
- Action Not Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask:

For the output data filters:

- Deny bounce back packet

All contents copyright © 2010 ZyXEL Communications Corporation.

- Allow packets that originate from us

Filter rule setup:

- Filter Type =TCP/IP Filter Rule
- Active =Yes
- Destination IP Addr =a.b.c.d
- Destination IP Mask =w.x.y.z
- Action Matched =Drop
- Action No Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask.

All contents copyright © 2010 ZyXEL Communications Corporation.

Product FAQ

1. What is SHDSL, SHDSL.bis?

SHDSL stands for Symmetric High-data-rate Digital Subscriber Line. SHDSL bases on TC-PAM (Trellis Coded Pulse Amplitude Modulation) which offers symmetrical transmission speed up to 2.30 Mbps (2-wire mode).

SHDSL.bis boots SHDSL performance to approximately 5.70 Mbps (2-wire mode) or 11.4 Mbps (4-wire mode).

2. How can I manage P-793H v2?

- Multilingual Embedded Web GUI for Local and Remote management
- SMT via console.
- Telnet support (Administrator Password Protected) for remote configuration change and status monitoring
- FTP/ TFTP sever, firmware upgrade and configuration backup and restore are supported (Administrator Password Protected)

3. What is the default password for Web Configurator?

There are two different accounts for P-793H v2 Web Configurator: **Common User Account** and **Administrator Account.**
By factory default the password for the two accounts are:

- Common User Account: **user**
- Administrator Account: **1234**.

You can change the password after you logging in the Web Configurator.
Note: By default, the password is “user”.

4. What’s the difference between ‘Common User Account’ and ‘Administrator Account’?

For Common User Account, it can only access the status monitor of P-793H v2 and check the current system status.

For Administrator Account, besides accessing the status monitor of P-793H v2, it can also access Wizard setup / Advanced setup of P-793H v2.

Moreover, only with Administrator Password, you could manage the P-793H v2 via FTP/TFTP or Telnet.

5. How do I know the P-793H v2's WAN IP address assigned by the ISP?

You can view **"IP Address: x.x.x.x"** shown in Web Configurator ‘**Status->Device Information ->WAN Information’**.

All contents copyright © 2010 ZyXEL Communications Corporation.

6. What do I need before using the SHDSL?

1. You must order the SHDSL service from your telephone company and choose the service category.
2. Your telephone company must have tested the phone line for the SHDSL transfer rate.
3. You must have subscribed to an ISP (Internet Service Provider) already and have the following information:

    - The user name and password for the connection
    - VPI/VCI number (Virtual Path Indentifier/Virtual Circuit Identifier) assigned by the Tele company.
    - The encapsulation protocol the service provider supports. It can be PPP, RFC 1483, or ENET ENCAP.
    - The DNS and gateway, and ENET ENCAP Gateway if the encapsulation is ENET ENCAP.

7. What should I do when the power (PWR) LED is off?

Make sure the P-793H v2 is connected to the power adapter, the power adapter is plugged into a power outlet and the power switch is at the ON position.

8. How to debug while DSL LED is off?

Check the connection between the P-793H v2's DSL port and the wall socket or remote devices. If you use the back to back application, check the service type and the Standard Mode in both P-793H v2s.

9. How do I verify my PC's IP address assigned by the P-793H v2?

Make sure you have the P-793H v2 powered on and then turn on your PC. After the PC starts, select " Run..." from the windows "Start" menu. Enter "cmd" and click OK. You may check IP of your PC with “ipconfig”. Verify your cabling if the IP address box shows "0.0.0.0".

10. What is Traffic Shaping?

Traffic Shaping is a feature in the P-793H v2. It allocates the bandwidth to WAN dynamically and aims at boosting the efficiency of the bandwidth. If there are several VCs in the P-793H v2 but only one VC activated at one time, the P-793H v2 allocates all the Bandwidth to the VC and the VC gets full bandwidth. If another VCs are activated later, the bandwidth is yield to other VCs after ward.

11. What do the parameters (PCR, SCR, MBS) mean?

All contents copyright © 2010 ZyXEL Communications Corporation.

Traffic shaping parameters (PCR, SCR, MBS) can be set in Menu 4 and Menu 11.6 and is valid for both incoming and outgoing direction since G.shdsl is symmetric.

Peak Cell Rate(PCR): The maximum bandwidth allocated to this connection. The VC connection throughput is limited by PCR.

Sustainable Cell Rate(SCR): The least guaranteed bandwidth of a VC. When there are multi-VCs on the same line, the VC throughput is guaranteed by SCR.

Maximum Burst Size(MBS): The amount of cells transmitted through this VC at the Peak Cell Rate before yielding to other VCs. Total bandwidth of the line is dedicated to single VC if there is only one VC on the line. However, as the other VC asking the bandwidth, the MBS defines the maximum number of cells transmitted via this VC with Peak Cell rate before yielding to other VCs.

The P-793H v2 holds the parameters for shaping the traffic among its virtual channels. If you do not need traffic shaping, please set SCR = 0, MBS = 0 and PCR as the maximum value according to the line rate (for example, 2.3 Mbps line rate will result PCR as 5424 cell/sec.)

12. What do ATM QoS Types (CBR, UBR, VBR-nRT, VBR-RT) mean?

Constant bit rate(CBR): An ATM bandwidth-allocation service that requires the user to determine a fixed bandwidth requirement at the time the connection is set up so that the data can be sent in a steady stream. CBR service is often used when transmitting fixed-rate uncompressed video.

Unspecified bit rate(UBR): An ATM bandwidth-allocation service that does not guarantee any throughput levels and uses only available bandwidth. UBR is often used when transmitting data that can tolerate delays, such as e-mail.

Variable bit rate(VBR): An ATM bandwidth-allocation service that allows users to specify a throughput capacity (i.e., a peak rate) and a sustained rate but data is not sent evenly. You can select VBR for busty traffic and bandwidth sharing with other applications. It contains two subclasses: Variable bit rate non real time (VBR-nRT) and Variable bit rate real time (VBR-RT).

13. Why do we perform traffic shaping in the P-793H v2?

The P-793H v2 must manage traffic fairly and provide bandwidth allocation for different sorts of applications, such as voice, video, and data. All applications have their own natural bit rate. Large data transactions have a fluctuating natural bit rate. The P-793H v2 is able to support variable traffic among different virtual connections. Certain traffic may be discarded if the virtual connection experiences congestion. Traffic shaping defines a set of actions taken by the

All contents copyright © 2010 ZyXEL Communications Corporation.

P-793H v2 to avoid congestion; traffic shaping takes measures to adapt to unpredictable fluctuations in traffic flows and other problems among virtual connections.

14. The P-793H v2 supports Bridge and Router mode, what's the difference between them?

When the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use bridge mode which works as a DSL modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to add another Internet sharing device, like a router. In this case, we use the router mode which works as a general Router plus a DSL Modem.

15. How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the P-793H v2 if the ISP uses PPPoE.

16. Why does my provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

17. What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as http://www.dyndns.org/.

Without DDNS, we always tell the users to use the WAN IP of the P-793H v2to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-793H v2, you apply a DNS name (e.g.,

All contents copyright © 2010 ZyXEL Communications Corporation.

www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-793H v2.

When the ISP assigns the P-793H v2 a new IP, the P-793H v2 updates this IP to DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

18. When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the P-793H v2 sends this IP to the DDNS server for its updates.

19. What is DDNS wildcard? Does the P-793H v2support DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the hostname, *.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

Yes, the P-793H v2 supports DDNS wildcard that http://www.dyndns.org/ supports. When using wildcard, you simply enter yourhost.dyndns.org in the Host field in Menu 1.1 Configure Dynamic DNS.

20. Can the P-793H v2's SUA handle IPSec packets sent by the IPSec gateway?

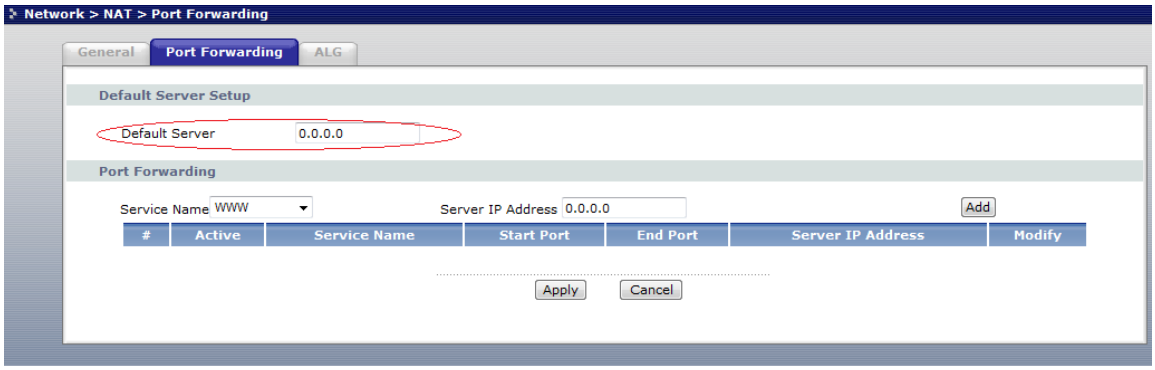
Yes, the P-793H v2's SUA can handle IPSec ESP Tunneling mode. We know when packets go through SUA, SUA will change the source IP address and source port for the host. To pass IPSec packets, SUA must understand the ESP packet with protocol number 50, replace the source IP address of the IPSec gateway to the router's WAN IP address. However, SUA should not change the source port of the UDP packets which are used for key managements. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

21. How do I setup my P-793H v2 for routing IPSec packets over SUA?

For outgoing IPSec tunnels, no extra setting is required.

All contents copyright © 2010 ZyXEL Communications Corporation.

For forwarding the inbound IPSec ESP tunnel, A 'Default' server set is required. You could configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding -> Default Server Setup:**



It is because SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP of this server in Web configurator. Thus SUA is able to forward the incoming packets to the requested service behind SUA and the outside users access the server using the P-793H v2's WAN IP address. So, we have to configure the internal IPsec client as a default server (unspecified service port) when it acts a server gateway.

22. What is VLAN?

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group called VLAN Group. A station can belong to more than one group.

The stations on the same VLAN group can communicate with each other. With VLAN, a station cannot directly talk to or hear from stations that are not in the same VLAN group(s); the traffic must first go through a router.

23. 802.1Q/1P

In order to resolve the limitation of port based VLAN, this framework of 802.1Q/1P feature is proposed. The key concepts are as below:

- One VLAN group is treated as “individual” device, just like there are many virtual devices on one physical device.
- Each LAN port, and PVC is similar to a VLAN switch port. Each can be grouped into any 802.1Q VLAN group and individually configured as tagged or untagged.
- The PVID of Each LAN port, and PVC can be individually configured.
- In each VLAN group, it is allowed to have multiple bridge PVCs, route PVCs or mixed PVCs.

All contents copyright © 2010 ZyXEL Communications Corporation.

24. What is Traffic Redirect ?

Traffic redirect forwards WAN traffic to a backup gateway when the Prestige cannot connect to the Internet through it's normal gateway. Thus make your backup gateway as an auxiliary backup of your WAN connection. Once Prestige detects its WAN connectivity is broken, Prestige will try to forward outgoing traffic to backup gateway that users specify in traffic redirect configuration menu.

25. What is Dial Backup?

It is Auto Fail-over and Fall-back WAN Backup Solution.

The P-793H v2 features a Fail-over and Fail-back WAN Backup Solution for complete reliability. When the DSL connection fails, traffic is forwarded to either a backup ISDN or analog modem to maintain data exchange. When the DSL connection is re-established, traffic will be fully restored. The WAN Backup Solution saves device maintenance cost and reduces loss from daily operation.

In addition, P-793H v2 also performs backup functions by redirecting traffic to a specific gateway to ensure availability of the Internet connection.

DSL FAQ

1. How does DSL compare to Cable modems?

DSL provides a dedicated service over a single telephone line; cable modems offer a dedicated service over a shared media. While cable modems have greater downstream bandwidth capabilities (up to 30 Mbps), that bandwidth is shared among all users on a line, and will therefore vary, perhaps dramatically, as more users in a neighborhood get online at the same time. Cable modem upstream traffic will in many cases be slower than DSL, either because the particular cable modem is inherently slower, or because of rate reductions caused by contention for upstream bandwidth slots. The big difference between DSL and cable modems, however, is the number of lines available to each. There are no more than 12 million homes passed today that can support

All contents copyright © 2010 ZyXEL Communications Corporation.

two-way cable modem transmissions, and while the figure also grows steadily, it will not catch up with telephone lines for many years. Additionally, many of the older cable networks are not capable of offering a return channel; consequently, such networks will need significant upgrading before they can offer high bandwidth services.

2. How do I know the DSL line is up?

You can see the DSL LEDs on the P-793H v2's front panel are on Green when the DSL physical layer is up.

Note: There are two DSL LEDs: DSL1 and DSL2.

When we use one line for Internet access or back to back application, DSL1 and DSL2 will act the same as one LED.

When we use 1-2 back to back application by Y cable, they will show the respective DSL line status.

3. How does the P-793H v2 work on a noisy DSL?

Depending on the line quality, the P-793H v2 uses "Fall Back" and "Fall Forward" to automatically adjust the date rate.

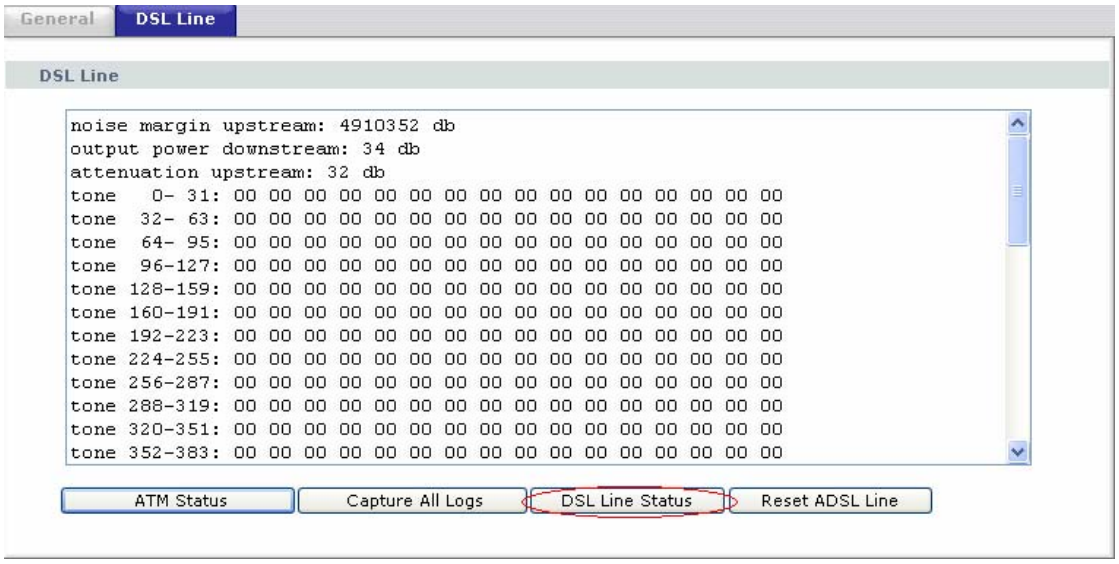
4. Does the VC-based multiplexing perform better than the LLC-based multiplexing?

Though the LLC-based multiplexing can carry multiple protocols over a single VC, it requires extra header information to identify the protocol being carried on the virtual circuit (VC). The VC-based multiplexing needs a separate VC for carrying each protocol but it does not need the extra headers. Therefore, the VC-based multiplexing is more efficient.

5. How do I know the details of my DSL line statistics?

In WEB Configurator**, Maintenance -> Diagnostic -> DSL Line -> DSL Line Status:**

All contents copyright © 2010 ZyXEL Communications Corporation.



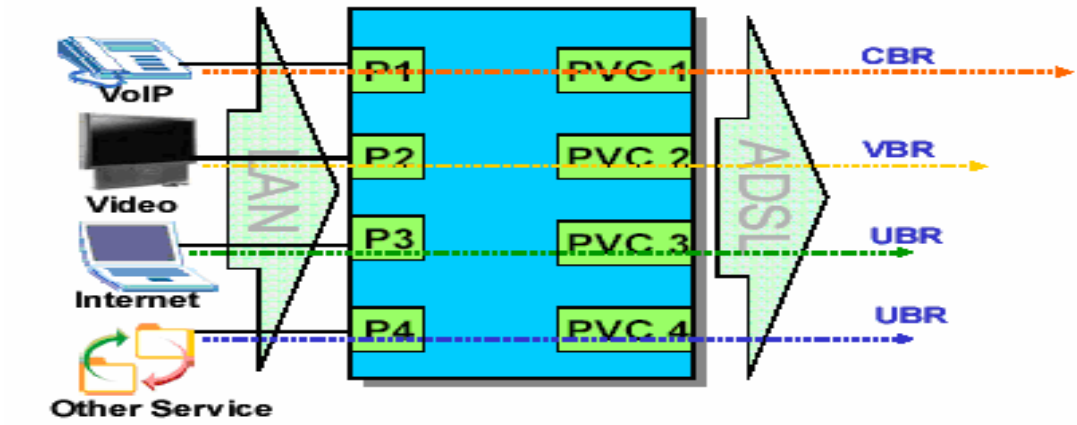
6. What are the signaling pins of the DSL connector?

The signaling pins on the P-793H v2's DSL connector RJ11 cable are pin 3 and 4 for 2-wire mode, and pin 2, 3, 4 and 5 for 4-wire mode.

7. What is triple play?

More and more Telco/ISPs are providing three kinds of services (VoIP, Video and Internet) over one existing DSL connection.

- The different services (such as video, VoIP and Internet access) require different Quality of Service.
- The high priority is Voice (VoIP) data.
- The Medium priority is Video (IPTV) data.
- The low priority is internet access such as ftp etc …



All contents copyright © 2010 ZyXEL Communications Corporation.

Triple Play is a VLAN-based policy to forward packets from LAN ports to different PVCs, thus you can configure each PVC separately to assign different QoS to different application.

Firewall FAQ

General

1. What is a network firewall?

A firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. The firewall can be thought of two mechanisms: One to block the traffic, and the other to permit traffic.

2. What makes P-793H v2 secure?

The P-793H v2 is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND attack, IP Spoofing, etc. It also uses stateful packet inspection to determine if an inbound connection is allowed through the firewall to the private LAN. The P-793H v2 supports Network Address Translation (NAT), which translates the private local addresses to one or multiple public addresses. This adds a level of security since the clients on the private LAN are invisible to the Internet.

3. What are the basic types of firewalls?

Conceptually, there are three types of firewalls:

1. Packet Filtering Firewall
2. Application-level Firewall
3. Stateful Inspection Firewall

Packet Filtering Firewalls generally make their decisions based on the header information in individual packets. These headers information include the source, destination addresses and ports of the packets.

All contents copyright © 2010 ZyXEL Communications Corporation.

Application-level Firewalls generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform logging and auditing of traffic passing through them. A proxy server is an application gateway or circuit-level gateway that runs on top of general operating system such as UNIX or Windows NT. It hides valuable data by requiring users to communicate with secure systems by mean of a proxy. A key drawback of this device is performance.

Stateful Inspection Firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also 'inspect' the session data to assure the integrity of the connection and to adapt to dynamic protocols. The flexible nature of Stateful Inspection firewalls generally provides the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support.

4. What kind of firewall is the P-793H v2?

1. The P-793H v2's firewall inspects packets contents and IP headers. It is applicable to all protocols, that understands data in the packet is intended for other layers, from network layer up to the application layer.
2. The P-793H v2's firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading
   as a response to a nonexistent outbound request can be blocked.
3. The 793H's firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
4. The P-793H v2's firewall is fast. It uses a hashing function to search the matched session cache instead of going through every individual rule for a packet.
5. The P-793H v2's firewall provides email service to notify you for routine reports and when alerts occur.

5. Why do you need a firewall when your router has packet filtering and NAT built-in?

With the spectacular growth of the Internet and online access, companies that do business on the Internet face greater security threats. Although packet filter and NAT restrict access to particular computers and networks.
However, for the other companies this security may be insufficient, because packets filters typically cannot maintain session state. Thus, for greater security, a firewall is considered.

All contents copyright © 2010 ZyXEL Communications Corporation.

6. What is Denials of Service (DoS) attack?

Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. There are four types of DoS attacks:

1. Those that exploits bugs in a TCP/IP implementation such as Ping of Death and Teardrop.
2. Those that exploits weaknesses in the TCP/IP specification such as SYN Flood and LAND Attacks.
3. Brute-force attacks that flood a network with useless data such as Smurf attack.
4. IP Spoofing

7. What is Ping of Death attack?

Ping of Death uses a 'PING' utility to create an IP packet that exceeds the maximum 65535 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang, or reboot.

8. What is Teardrop attack?

Teardrop attack exploits weakness in the reassemble of the IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original packet except that it contains an offset field. The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

9. What is SYN Flood attack?

SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set a relatively long intervals) terminates the TCP three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

All contents copyright © 2010 ZyXEL Communications Corporation.

10. What is LAND attack?

In a LAN attack, hackers flood SYN packets to the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

11 What is Brute-force attack?

A Brute-force attack, such as 'Smurf' attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request packet, the resulting ICMP traffic will not only clog up the 'intermediary' network, but will also congest the network of the spoofed source IP address, known as the 'victim' network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

12. What is IP Spoofing attack?

Many DoS attacks also use IP Spoofing as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP Spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall.

13. What are the default ACL firewall rules in P-793H v2?

There are two default ACLs pre-configured in the P-793H v2, one allows all connections from LAN to WAN and the other blocks all connections from WAN to LAN except of the DHCP packets.

Configuration

1. How do I configure the firewall?

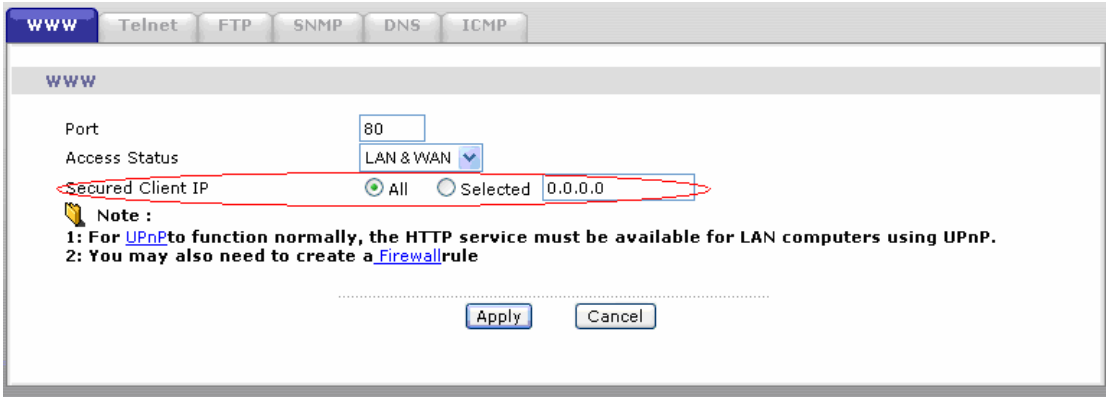
You can use the Web Configurator to configure the firewall for P-793H v2. By factory default, if you connect your PC to the LAN Interface of P-793H v2, you can access Web Configurator via ‘http://192.168.1.1’.

All contents copyright © 2010 ZyXEL Communications Corporation.

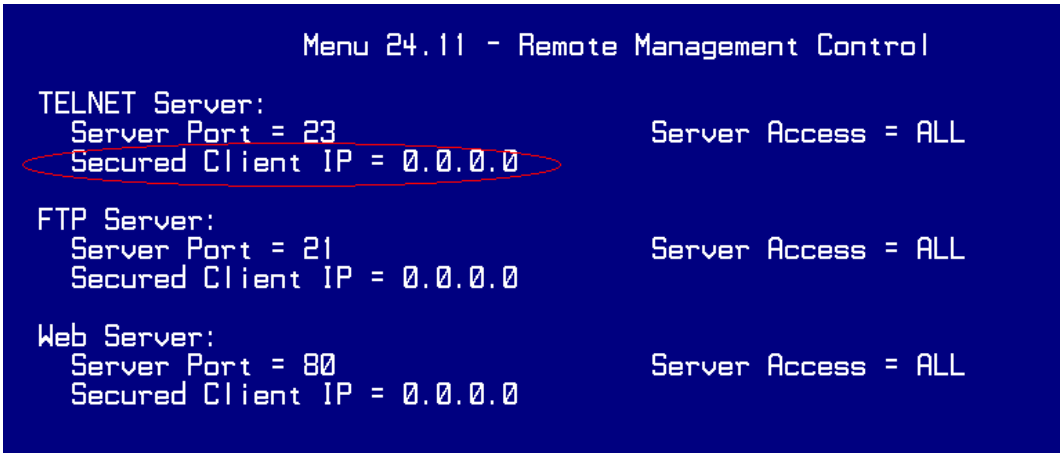
2. How do I prevent others from configuring my firewall?

There are several ways to protect others from touching the settings of your firewall.

1. Change the default Administrator password since it is required when setting up the firewall using Telnet, Console or Web browser.
2. Limit who can telnet to your P-793H v2 or access P-793H v2's Web Configurator. You can enter the IP address of the secured LAN host in Web Configurator, Advanced Setup, Advanced -> Remote MGNT -> [Service] ->Secured Client IP to allow special access to your P-793H v2:



The default value in this field is 0.0.0.0, which means you do not care which host is trying to telnet your P-793H v2 or access the Web Configurator of Plus: Above configuration can also be realized via SMT menu 24.11 as below:



3. Why can't I configure my P-793H v2 using Web Configurator/Telnet over WAN?

There are four reasons that WWW/Telnet from WAN is blocked.

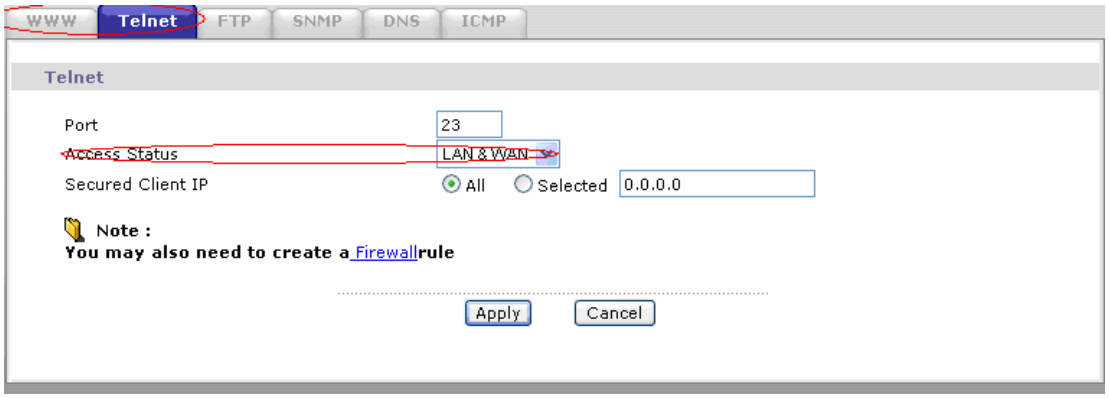
All contents copyright © 2010 ZyXEL Communications Corporation.

(1) When the firewall is turned on, all connections from WAN to LAN are blocked by the default ACL rule. To enable WWW/Telnet from WAN, you must turn the firewall off, or create a firewall rule to allow WWW/Telnet connection from WAN. The WAN-to-LAN ACL summary will look like as shown below.

WWW:
Source IP= Remote trusted host
Destination IP= router' WAN IP
Service= TCP/80
Action=Forward

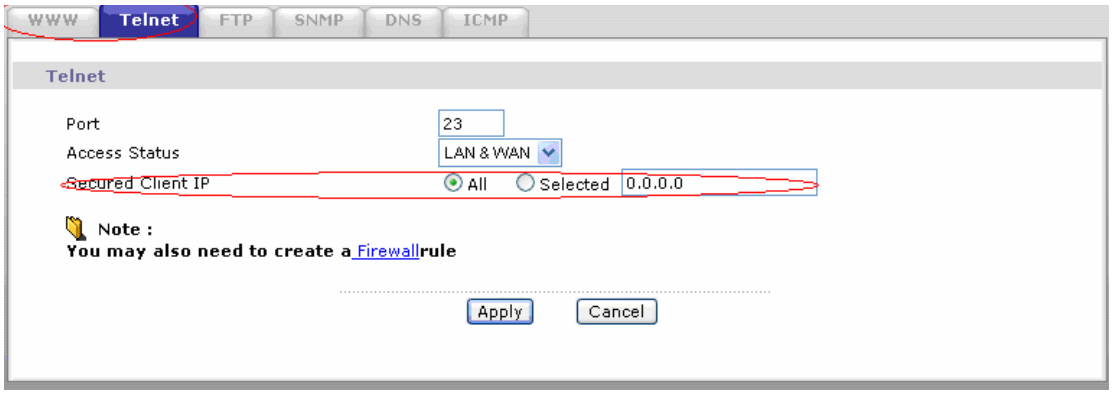
TELNET:
Source IP= Telnet Client host
Destination IP= router' WAN IP
Service= TCP/23
Action=Forward

(2)You have disabled WWW/Telnet service in SMT menu 24.11 or in Web Configurator, Advanced setup, **Advanced -> Remote MGNT:**



(3) WWW/Telnet service is enabled but your host IP is not the secured host entered in SMT menu 24.11 or in Web Configurator, Advanced setup, **Advanced -> Remote MGNT:**

All contents copyright © 2010 ZyXEL Communications Corporation.



(4)A filter set which blocks WWW/Telnet from WAN is applied to WAN node. The default filter rule 3 (Telnet_FTP_WAN) is applied in the Input Protocol field in menu 11.5.

4. Why can't I upload the firmware and configuration file using FTP over WAN?

(1) When the firewall is turned on, all connections from WAN to LAN are blocked by the default ACL rule. To enable FTP from WAN, you must turn the firewall off (Menu 21.2) or create a firewall rule to allow FTP connection from WAN. The WAN-to-LAN ACL summary will look like as shown below.

Source IP= FTP host
Destination IP= P-793H v2's WAN
IP Service= FTP TCP/21, TCP/20
Action=Forward

(2) You have disabled FTP service in Menu 24.11 or in Web Configurator, Advanced setup, **Advanced -> Remote MGNT.**

(3) FTP service is enabled but your host IP is not the secured host entered in SMT menu 24.11 or in Web Configurator, Advanced setup, **Advanced -> Remote MGNT.**

(4) A filter set which blocks FTP from WAN is applied to WAN node. The default filter rule 3 (Telnet_FTP_WAN) is applied in the Input Protocol field in menu 11.5.

Log and Alert

1. When does the P-793H v2 generate the firewall log?

All contents copyright © 2010 ZyXEL Communications Corporation.

The P-793H v2 generates the firewall log immediately when the packet matches a firewall rule. The log for Default Firewall Policy (LAN to WAN, WAN to LAN, WAN to WAN) is generated automatically with factory default setting, but you can customize it in Web Configurator, Advanced setup, **Maintenance -> Logs ->Log Settings.**

2. What does the log show to us?

The log supports up to 128 entries. There are 5 columns for each entry. Please see the example shown below:

#	Time	Message	Source	Destination	Notes
1	12/13/2005 15:35:21	Firewall default policy: TCP (L to W)	192.168.1.33:3466	207.69.188.186:5000	ACCESS PERMITTED

3. How do I view the firewall log?

All logs generated in P-793H v2, including firewall logs, IPSec logs, system logs are migrated to centralized logs. So you can view firewall logs in Centralized logs: Web Configurator, Advanced setup, **Maintenance -> Logs ->View Log.**

The log keeps 128 entries, the new entries will overwrite the old entries when the log has over 128 entries.

Before you can view firewall logs, there are two steps you need to do:
(1) Enable log function in Centralized logs setup via either one of the following methods,

- Web configuration: Advanced Setup, **Maintenance -> Logs -> Log Settings**, **"Active Log and Alert"** check options depending on your real situation.
- CI command: **sys logs category [access | attack]**

(2) Enable log function in firewall default policy or in firewall rules.

After the above two steps, you can view firewall logs via

- Web Configurator: Advanced setup, **Maintenance -> Logs ->View Log.**
- View the log by CI command: **sys logs disp**

You can also view Centralized logs via **mail** or **syslog**, please configure mail server or Unix Syslog server in Web configuration: Advanced Setup, **Maintenance -> Logs -> Log Settings**.

All contents copyright © 2010 ZyXEL Communications Corporation.

4. When does the P-793H v2 generate the firewall alert?

The P-793H v2 generates the alert when an attack is detected by the firewall and sends it via Email. So, to send the alert, you must configure the mail server and Email address using Web Configurator, Advanced Setup, **Maintenance -> Logs -> Log Settings**. You can also specify how frequently you want to receive the alert in it.

5. What is the difference between the log and alert?

A log entry is just added to the log inside the P-793H v2 and e-mailed together with all other log entries at the scheduled time as configured. An alert is e-mailed immediately after an attacked is detected.

IPSec FAQ

VPN Overview

1. What is VPN?

A VPN gives users a secure link to access corporate network over the Internet or other public or private networks without the expense of lease lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

2. Why do I need VPN?

There are some reasons to use a VPN. The most common reasons are because of security and cost.

Security

(1). Authentication

With authentication, VPN receiver can verify the source of packets and guarantee the data integrity.

(2). Encryption

With encryption, VPN guarantees the confidentiality of the original user data.

Cost

(1). Cut long distance phone charges

All contents copyright © 2010 ZyXEL Communications Corporation.

Because users typically dial the their local ISP for VPN, thus, long distance phone charge is reduced than making a long direct connection to the remote office.

(2).Reducing number of access lines

Many companies pay monthly charges for two types access lines: (1) high-speed links for their Internet access and (2) frame relay, ISDN Primary Rate Interface or T1 lines to carry data. A VPN may allow a company to carry the data traffic over its Internet access lines, thus reducing the need for some installed lines.

3. What are most common VPN protocols?

There are currently three major tunneling protocols for VPNs. They are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec).

4. What is PPTP?

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself. The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

5. What is L2TP?

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

6. What is IPSec?

IPSec is a set of IP extensions developed by IETF (Internet Engineering Task Force) to provide security services compatible with the existing IP standard (IPv4) and also the upcoming one (IPv6). In addition, IPSec can protect any protocol that runs on top of IP, for instance TCP, UDP, and ICMP. The IPSec provides cryptographic security services. These services allow for authentication, integrity, access control, and confidentiality. IPSec allows for the information exchanged between remote sites to be encrypted and verified. You can create encrypted tunnels (VPNs), or just do encryption between computers. Since you have so many options, IPSec is truly the most extensible and complete network security solution.

7. What secure protocols does IPSec support?

All contents copyright © 2010 ZyXEL Communications Corporation.

There are two protocols provided by IPSec, they are AH (Authentication Header, protocol number 51) and ESP (Encapsulated Security Payload, protocol number 50).

8. What are the differences between 'Transport mode' and 'Tunnel mode?

The IPSec protocols (AH and ESP) can be used to protect either an entire IP payload or only the upper-layer protocols of an IP payload. Transport mode is mainly for an IP host to protect the data generated locally, while tunnel mode is for security gateway to provide IPSec service for other machines lacking of IPSec capability.

In this case, Transport mode only protects the upper-layer protocols of IP payload (user data). Tunneling mode protects the entire IP payload including user data.

There is no restriction that the IPSec hosts and the security gateway must be separate machines. Both IPSec protocols, AH and ESP, can operate in either transport mode and tunnel mode.

9. What is SA?

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

10. What is IKE?

IKE is short for Internet Key Exchange. Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration to set up a VPN.

There are two phases in every IKE negotiation- phase 1 (Authentication) and phase 2 (Key Exchange). Phase 1 establishes an IKE SA and phase 2 uses that SA to negotiate SAs for IPSec.

11. What is Pre-Shared Key?

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called 'Pre-shared' because you have to share it with another party before you can communicate with them over a secure connection.

12. What are the differences between IKE and manual key VPN?

The only difference between IKE and manual key is how the encryption keys and SPIs are determined.

All contents copyright © 2010 ZyXEL Communications Corporation.

For IKE VPN, the key and SPIs are negotiated from one VPN gateway to the other. Afterward, two VPN gateways use this negotiated keys and SPIs to send packets between two networks.

For manual key VPN, the encryption key, authentication key (if needed), and SPIs are predetermined by the administrator when configuring the security association.

IKE is more secure than manual key, because IKE negotiation can generate new keys and SPIs randomly for the VPN connection.

13. What is Phase 1 ID for?

In IKE phase 1 negotiation, IP address of remote peer is treated as an indicator to decide which VPN rule must be used to serve the incoming request. However, in some application, remote VPN box or client software is using an IP address dynamically assigned from ISP, so P-793H v2 needs additional information to make the decision. Such additional information is what we call phase 1 ID. In the IKE payload, there are local and peer ID field to achieve this.

14. What is FQDN?

FQDN(Fully Qualified Domain Name), IKE standard takes it as one type of Phase 1 ID.

As we mentioned, Phase 1 ID is an identification for each VPN peer. The type of Phase 1 ID may be IP/FQDN(DNS)/User FQDN(E-mail). The content of Phase 1 ID depends on the Phase 1 ID type. The following is an example for how to configure phase 1 ID.

ID type Content

IP 202.132.154.1
DNS www.zyxel.com
E-mail support@zyxel.com.tw

Please note that, in P-793H v2, if "DNS" or "E-mail" type is chosen, you can still use a random string as the content, such as "this_is_P-793H v2". It's not necessary to follow the format exactly.

By default, P-793H v2 takes IP as phase 1 ID type for itself and it's remote peer. But if it's remote peer is using DNS or E-mail, you have to adjust the settings to pass phase 1 ID checking.

All contents copyright © 2010 ZyXEL Communications Corporation.

15. When should I use FQDN?

If your VPN connection is P-793H v2 to P-793H v2, and both of them have static IP address, and there is no NAT router in between, you can ignore this option. Just leave Local/Peer ID type as IP, then skip this option.

If either side of VPN tunneling end point is using dynamic IP address, you may need to configure ID for the one with dynamic IP address. And in this case, "Aggressive mode" is recommended to be applied in phase 1 negotiation .

P-793H v2 VPN

1. How do I configure P-793H v2 VPN?

You can configure P-793H v2 for VPN using SMT or Web configurator.

2. What VPN protocols are supported by P-793H v2?

P-793H v2 supports ESP (protocol number 50) and AH (protocol number 51).

3. What types of authentication does P-793H v2 VPN support?

VPN vendors support a number of different authentication methods. P-793H v2 VPN supports both SHA1 and MD5.

AH provides authentication, integrity, and replay protection (but not confidentiality). Its main difference with ESP is that AH also secures parts of the IP header of the packet (like the source/destination addresses), but ESP does not.

ESP can provide authentication, integrity, replay protection, and confidentiality of the data (it secures everything in the packet that follows the header). Replay protection requires authentication and integrity (these two go always together). Confidentiality (encryption) can be used with or without authentication/integrity. Similarly, one could use authentication/integrity with or without confidentiality.

4. I am planning my P-793H v2-to-P-793H v2 VPN configuration. What do I need to know?

First of all, both P-793H v2s must have VPN capabilities.

All contents copyright © 2010 ZyXEL Communications Corporation.

If your P-793H v2 is capable of VPN, you can find the VPN options in Advanced>VPN tab.

For configuring a 'box-to-box VPN', there are some tips:

1. If there is a NAT router running in the front of P-793H v2, please make sure the NAT router supports to pass through IPSec.
2. In NAT case (either run on the frond end router, or in P-793H v2 VPN box), only IPSec ESP tunneling mode is supported since NAT againsts AH mode.
3. **Source IP/Destination IP**Please do not number the LANs (local and remote) using the same exact range of private IP addresses. This will make VPN destination addresses and the local LAN addresses are indistinguishable, and VPN will not work.
4. **Secure Gateway IP Address** This must be a public, routable IP address, private IP is not allowed. That means it can not be in the 10.x.x.x subnet, the 192.168.x.x subnet, nor in the range 172.16.0.0 - 172.31.255.255 (these address ranges are reserved by internet standard for private LAN numberings behind NAT devices). It is usually a static IP so that we can pre-configure it in P-793H v2 for making VPN connections. If it is a dynamic IP given by ISP, you still can configure this IP address after the remote P-793H v2 is on-line and its WAN IP is available from ISP.

5. Does P-793H v2 support dynamic secure gateway IP?

If the remote VPN gateways use dynamic IP, we enter **0.0.0.0** as the **Secure Gateway IP Address** in P-793H v2. In this case, the VPN connection can only be initiated from dynamic side to fixed side in order to update its dynamic IP to the fixed side. However, if both gateways use dynamic IP addresses, it is no way to establish VPN connection at all.

6. What VPN gateway that has been tested with P-793H v2 successfully?

We have tested P-793H v2 successfully with the following third party VPN gateways.

- Cisco 1720 Router, IOS 12.2(2)XH, IP/DSL/FW/IDS PLUS IPSEC 3DES
- NetScreen 5, ScreenOS 2.6.0r6
- SonicWALL SOHO 2
- WatchGuard Firebox II
- ZyXEL P-793H v2
- Avaya VPN

All contents copyright © 2010 ZyXEL Communications Corporation.

- Netopia VPN
- Ill VPN

7. What VPN software that has been tested with P-793H v2 successfully?

We have tested P-793H v2 successfully with the following third party VPN software.

- SafeNet Soft-PK, 3DES edition
- Checkpoint Software
- SSH Sentinel, 1.4
- SecGo IPSec for Windows
- F-Secure IPSec for Windows
- KAME IPSec for UNIX
- Nortel IPSec for UNIX
- Intel VPN, v. 6.90
- FreeS/WAN for Linux
- SSH Remote ISAKMP Testing Page, (http://isakmp-test.ssh.fi/cgi-bin/nph-isakmp-test)
- Windows 2000, IPSec

8. Is the host behind NAT allowed to use IPSec?

NAT Condition	Supported IPSec Protocol
VPN Gateway embedded NAT	AH tunnel mode, ESP tunnel mode
VPN client/gateway behind NAT*	ESP tunnel mode
NAT in Transport mode	None

The NAT router must support IPSec pass through. For example, for P-793H v2 SUA/NAT routers. The default port and the client IP have to be specified in menu 15-SUA Server Setup.

All contents copyright © 2010 ZyXEL Communications Corporation.

9. How do I configure P-793H v2 with NAT for internal servers?

Generally, without IPSec, to configure an internal server for outside access, we need to configure the server private IP and its service port in SUA/NAT Server Table.

However, if both NAT and IPSec is enabled in P-793H v2, the edit of the table is necessary only if the connection is a non-secure connections. For secure connections, none SUA server settings are required since private IP is reachable in the VPN case.

For example:

host----P-793H v2(NAT)----DSL Modem----Internet----Secure host
\
\
Non-secure host

10. I am planning my P-793H v2 behind a NAT router. What do I need to know?

Some tips for this:

The NAT router must support to pass through IPSec protocol. Only ESP tunnel mode is possible to work in NAT case. In the NAT router is P-793H v2 NAT router supporting IPSec pass through, default port and the P-793H v2 WAN IP must be configured in SUA/NAT Server Table.

1. WAN IP of the NAT router is the tunneling endpoint for this case, not the WAN IP of P-793H v2.
2. If firewall is turned on in P-793H v2, you must forward IKE port in Internet interface.
3. If NAT are also enabled in P-793H v2, NAT server is required for non-secure connections, NAT server is not required for secure connections and the physical private IP is used.

For example:

host----P-793H v2----NAT Router----Internet----Secure host
\

All contents copyright © 2010 ZyXEL Communications Corporation.

\
Non-secure host

11. How can I keep a tunnel alive?

To keep a tunnel alive, you can check "keep alive" option when configuring your VPN tunnel. With this option, whenever phase 2 SA lifetime is due, IKE negotiation procedure will be invoked automatically even without traffic to make the connection stay.

But to reduce the consumption of system resource, if VPN tunnels get disconnected either manually, by idle timer, or because of power cycle, packet triggering is still necessary to make the tunnel up.

12. Single, Range, Subnet, which types of IP address do P-793H v2 support in VPN/IPSec?

The mentioned P-793H v2 series support all of the types. In other words, you can specify a single PC, a range of PCs or even a network of PCs to utilize the VPN/IPSec service.

13. Can P-793H v2 support IPSec passthrough?

Yes, P-793H v2 can support IPSec passthrough. P-793H v2 series don't only support IPSec/VPN gateway, it can also be a NAT router supporting IPSec passthrough.

If the VPN connection is initiated from the security gateway behind P-793H v2, no configuration is necessary for NAT nor Firewall.

If the VPN connection is initiated from the security gateway outside of P-793H v2, NAT port forwarding and Firewall forwarding are necessary.

To configure NAT port forwarding, please go to WEB interface, Setup/ "SUA/NAT", put the secure gateway's IP address in default server.

To configure Firewall forwarding, please go to WEB interface, Setup/Firewall, select Packet Direction to WAN to LAN, and create a firewall rule the forwards IKE(UDP:500).

14. Can P-793H v2 behave as a NAT router supporting IPSec passthrough and an IPSec gateway simultaneously?

No, P-793H v2 can't support them simultaneously. You need to choose either one. If P-793H v2 is to support IPSec passthrough, you have to disable the VPN

All contents copyright © 2010 ZyXEL Communications Corporation.

function on P-793H v2. To disable it, you can either deactivate each VPN rule or issue a CI command, "ipsec switch off" from SMT menu 24.8. You can get into SMT menu via either telnet or console connection.

15. How do I use PTM Transfer Mode?

P-793H v2 supports ENET, PPPOE and RFC1483 encapsulation. Following original design, P-793H v2 supports 8 remote nodes, and each remote node is separated by VLAN ID.

All contents copyright © 2010 ZyXEL Communications Corporation.

Application Notes

General Application Notes

1. Internet Access Using P-793H v2 under Bridge mode

- Setup your workstation
- Setup your P-793H v2 under bridge mode

If the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use P-793H v2 which works as an DSL bridge modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

Set up your workstation

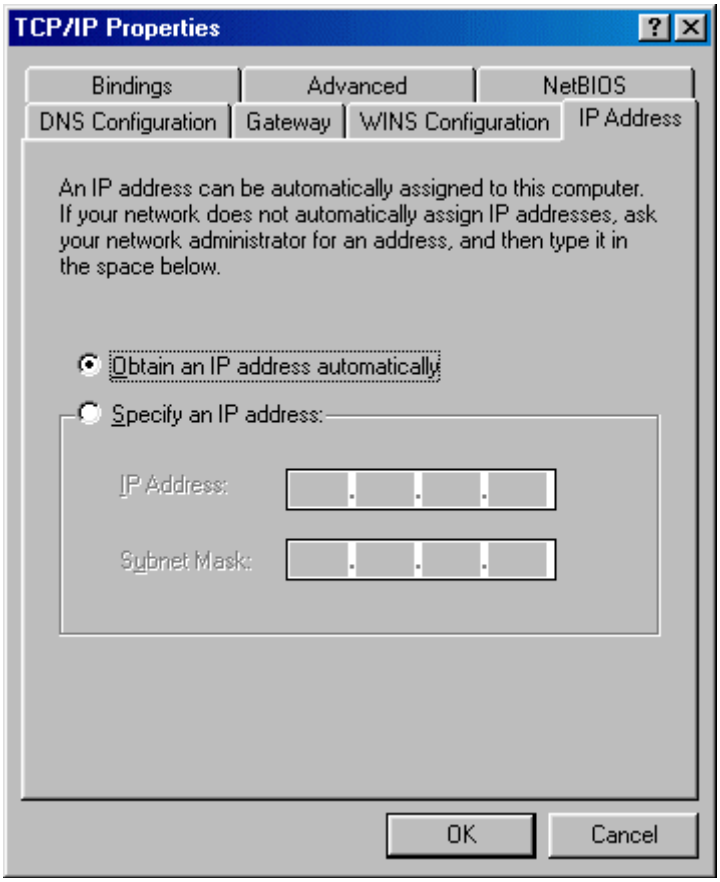
(1) Ethernet connection

To connect your computer to the P-793H v2's LAN port, the computer must have an Ethernet adapter card installed. For connecting a single computer to the P-793H v2, we use an Ethernet cable.

(2) TCP/IP configuration

In most cases, the IP address of computer is assigned by ISP dynamically so you have to configure the computer as a DHCP client which obtains the IP from the ISP using DHCP protocol. The ISP may also provide the gateway, DNS via DHCP if they are available. Otherwise, please enter the static IP addresses for all that the ISP gives to you in the network TCP/IP settings. For Windows, we check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup, please see the example shown below.

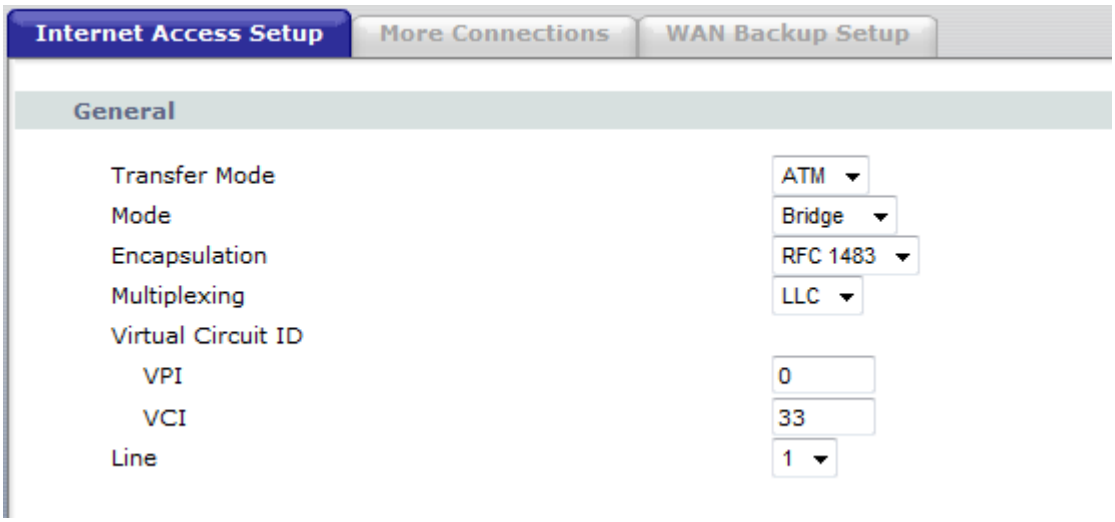
All contents copyright © 2010 ZyXEL Communications Corporation.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Setup your P-793H v2

The following procedure shows you how to configure your P-793H v2 as bridge mode. We will use Web Configurator to guide you through the related menu.

(1) Configure P-793H v2 as bridge mode and configure Internet setup parameters in Web Configurator, Advanced Setup, **Network -> WAN -> Internet Connection.**



All contents copyright © 2010 ZyXEL Communications Corporation.

Key Settings:

Option	Description
Transfer Mode	Select the correct Transfer Mode that your ISP supports. For example, ATM.
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.

(2) Turn off DHCP Server and configure a LAN IP for the P-793H v2 in Web Configurator, **Advanced Setup**, **Network -> LAN**. We use 192.168.1.1 as the LAN IP for P-793H v2 in this case:

Step 1: Inactivate DHCP Server and apply.

Step 2: Assign an IP to the LAN Interface of P-793H v2, e.g.192.168.1.1

2. Internet Access Using P-793H v2 under Routing mode

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to install an Internet sharing device, like a router. In this case, we use the P-793H v2 which works as a general Router plus a DSL Modem.

Set up your workstation

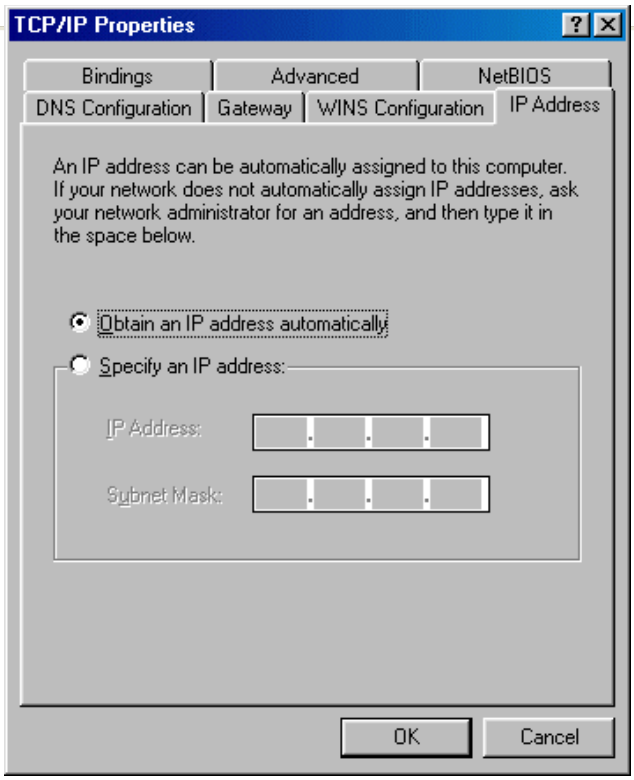
(1) Ethernet connection

Connect the LAN ports of all computers to the LAN Interface of P-793H v2 using Ethernet cables.

(2) TCP/IP configuration

Since the P-793H v2 is set to DHCP server as default, so you need only to configure the workstations as the DHCP clients in the networking settings. In this case, the IP address of the computer is assigned by the P-793H v2. The P-793H v2 can also provide the DNS to the clients via DHCP if it is available. For this setup in Windows, we check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup. Please see the example shown below.

All contents copyright © 2010 ZyXEL Communications Corporation.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Set up your P-793H v2 under routing mode

The following procedure shows you how to configure your P-793H v2 as Routing mode for routing traffic. We will use Web Configurator to guide you through related menu.

(1) Configure P-793H v2 as routing mode and configure Internet setup parameters in Web Configurator, Advanced Setup, **Network -> WAN -> Internet Connection.**

Key Settings:

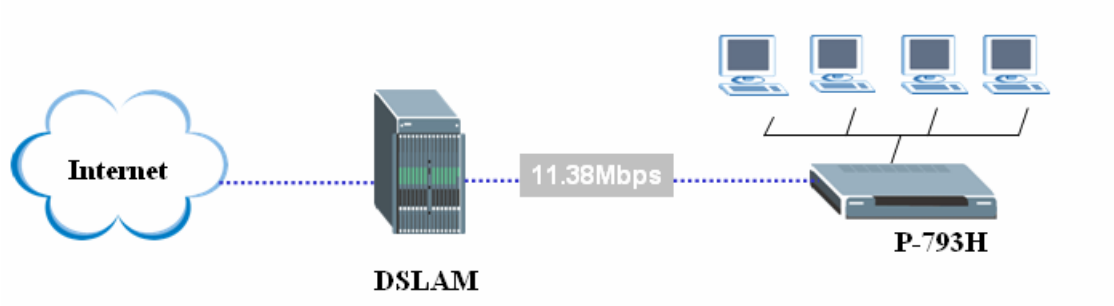
Option	Description
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.
IP Address Assignment	Set to **Dynamic** if the ISP provides the IP for the P-793H v2dynamically. Otherwise, set to **Static** and enter the IP in the **IP**
Service Type	Set options like “Service Mode” “Service Type” “Enable Rate Adaption” “Transfer Max Rate” “Transfer Min Rate” and “Standard Mode”.

All contents copyright © 2010 ZyXEL Communications Corporation.

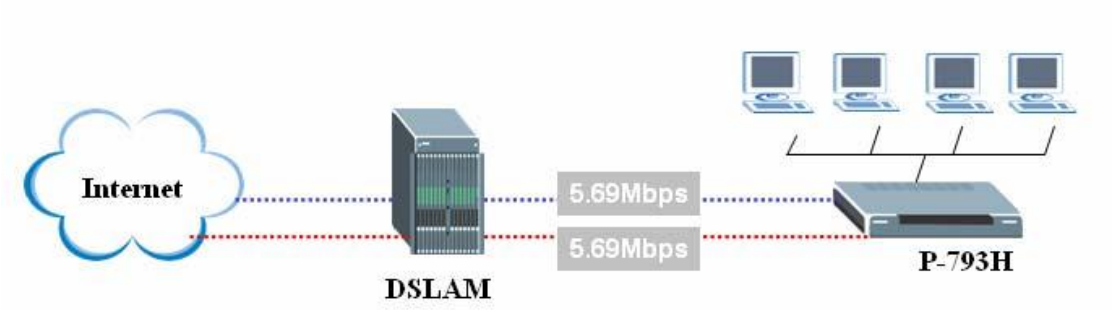
(2) Configure a LAN IP for the P-793H v2 and the DHCP settings in Web Configurator, **Advanced Setup**, **Network -> LAN.**

3. Internet Access scenarios

- **4 Wire Application**



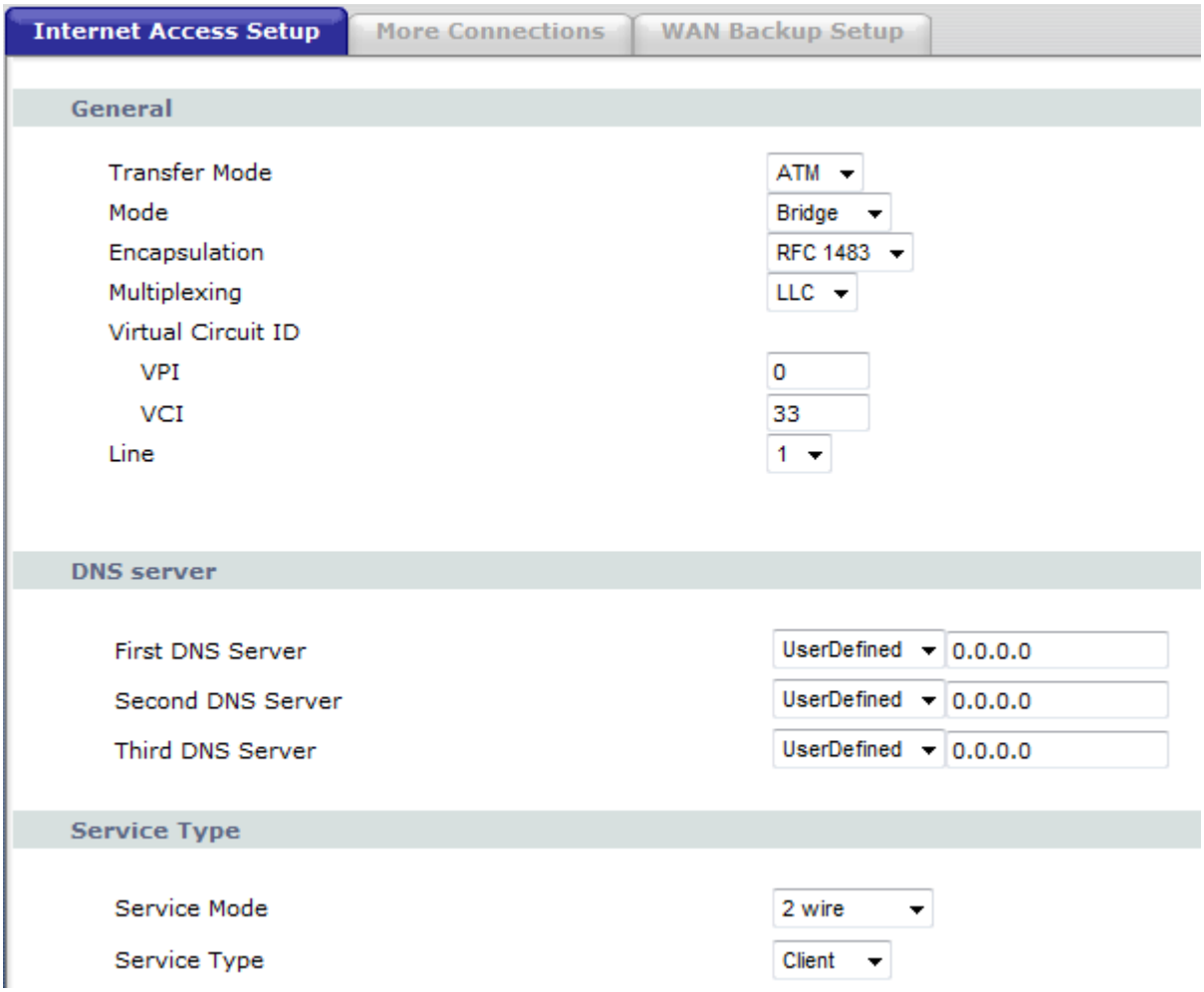
- **2 Wire Application**



Configuration Guide:

In WEB Configurator, **Network ⇗ WAN ⇗ Internet Connection,** there are three sets of settings: **General, IP Address, and Service Type.**

All contents copyright © 2010 ZyXEL Communications Corporation.

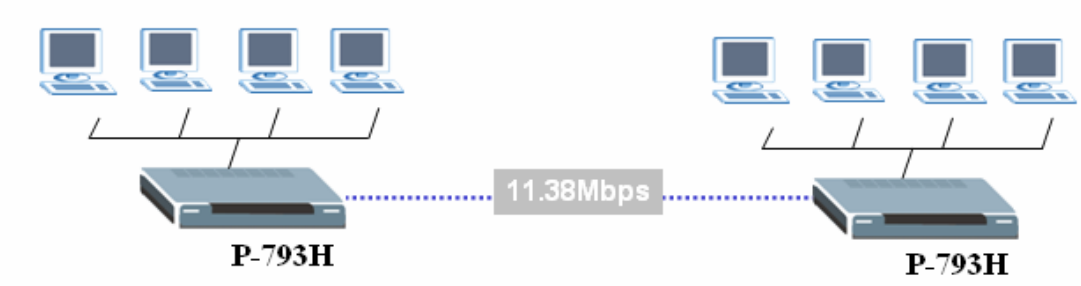


Please set proper parameter for your Internet Access.

4. Back to back scenarios

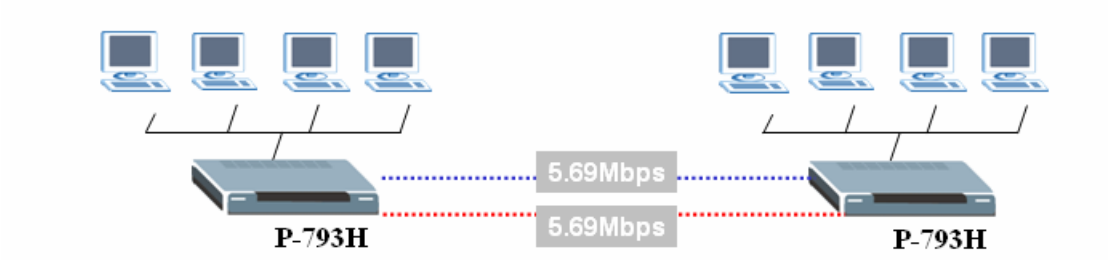
1 - 1 back to back

(1) 4 Wire Application

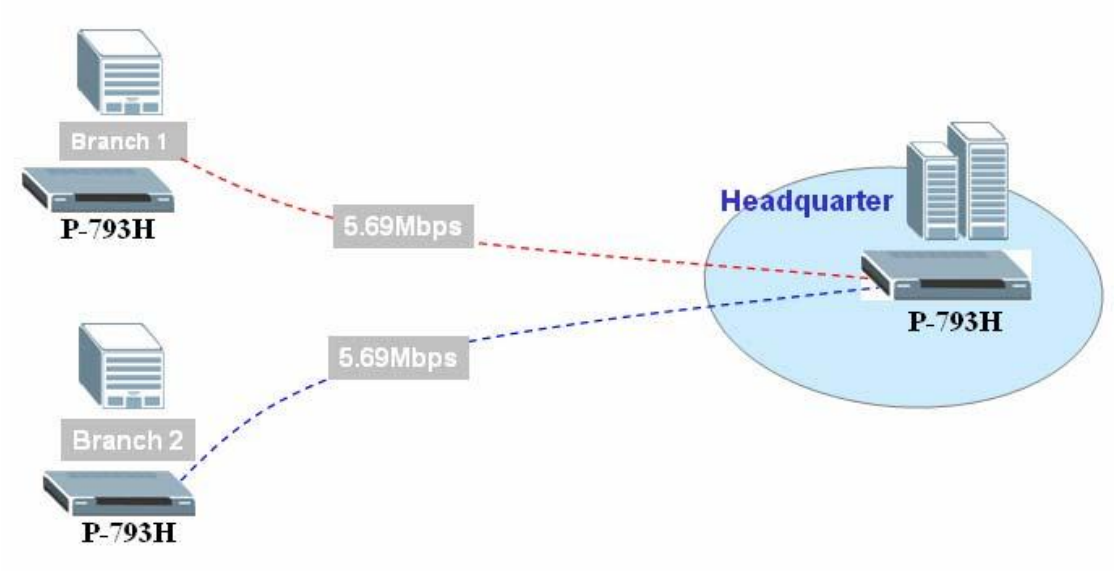


(2) 2 Wire Application

All contents copyright © 2010 ZyXEL Communications Corporation.



- **1 - 2 back to back**



Note 1: It is also compatible with G.SHDSL 2.3Mbps application when we connect it with P-792H or P-791R.

Note2 : There are two DSL led: DSL1 and DSL2.

When we use one line for Internet access or back to back application, DSL1 and DSL2 will act the same as one LED.

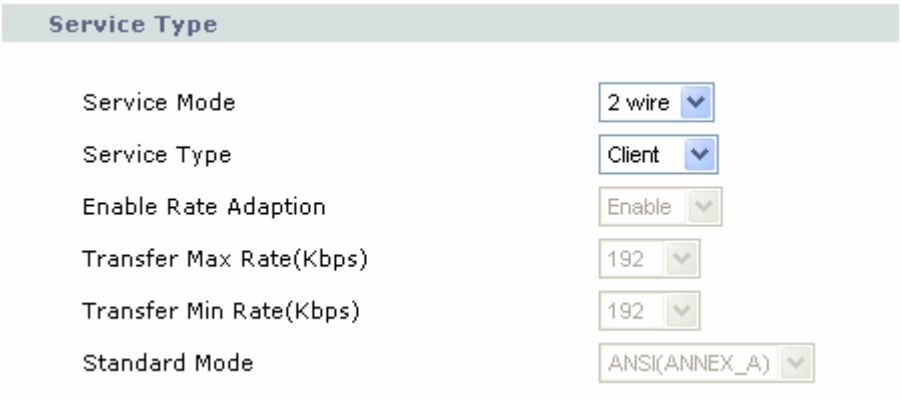
When we use 1-2 back to back application by Y cable, they will show the respective DSL line status.

5. What is the checklist for making a 1-1 Back-to-Back connection over P-793H v2?

1. Make sure one of the two P-793H v2s is with Service Type = Client, and the other one is with Service Type = Server.
2. The "Encapsulation", "Multiplexing", "VPI/VCI" option in menu 11 must be the same for both P793Hs.
3. Enter the remote IP address.

All contents copyright © 2010 ZyXEL Communications Corporation.

Note: When P-793H v2 works as client, options “Enable Rate Adaption” “Transfer Max Rate” “Transfer Min Rate” and “Standard Mode” are not available to choose. These parameters are then determined by server side.



6. What is the checklist for making a 1-2 Back-to-Back connection over P-793H v2?

1. Make sure the two remote P-793H v2s are with Service Mode=2 wire, and Service Type = Client. The central one is with Service Mode=4 wire, and Service Type = Server.
2. The "Encapsulation", "Multiplexing", "VPI/VCI" option in menu 11 must be the same for all P-793H v2s.
3. Enter the remote IP following: Remote ones take central one as gateway.

Note: This application is realized via One Y cable.(On the Y cable, there should be “DSL1” and “DSL2” printed on the offshoot phone cable which guide you to connect two clients)

7. Setup the P-793H v2 as a DHCP Relay

- **What is DHCP Relay?**

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P-793H v2 supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the LAN clients. When it is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 1.

All contents copyright © 2010 ZyXEL Communications Corporation.

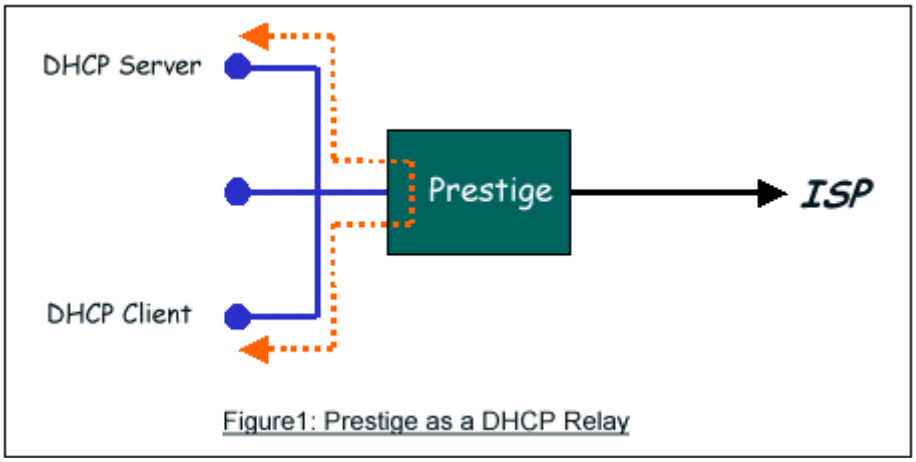
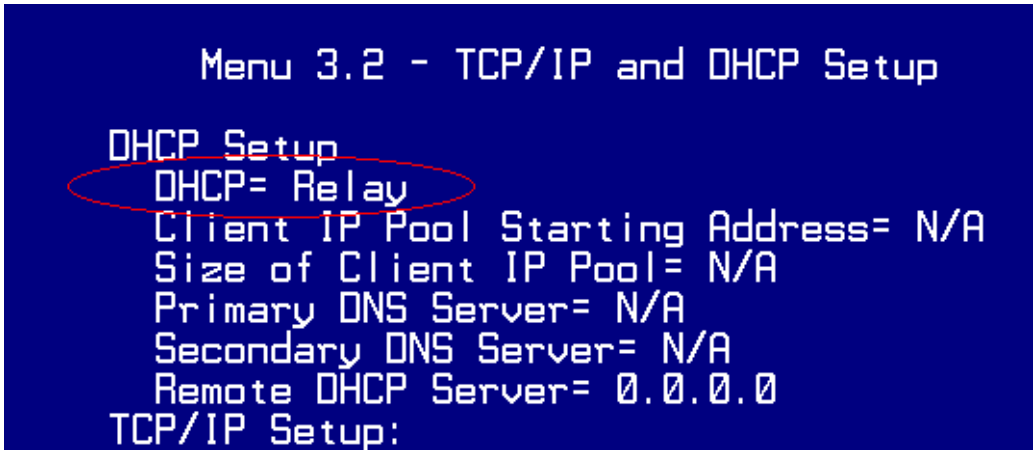


Figure1: Prestige as a DHCP Relay

- **Setup the P-793H v2 as a DHCP Relay**

We could set the P-793H v2 as a DHCP Relay via menu 3.2 as below:


Menu 3.2 - TCP/IP and DHCP Setup
DHCP Setup
DHCP= Relay
Client IP Pool Starting Address= N/A
Size of Client IP Pool= N/A
Primary DNS Server= N/A
Secondary DNS Server= N/A
Remote DHCP Server= 0.0.0.0
TCP/IP Setup:

Or via the following command in **CLI**:

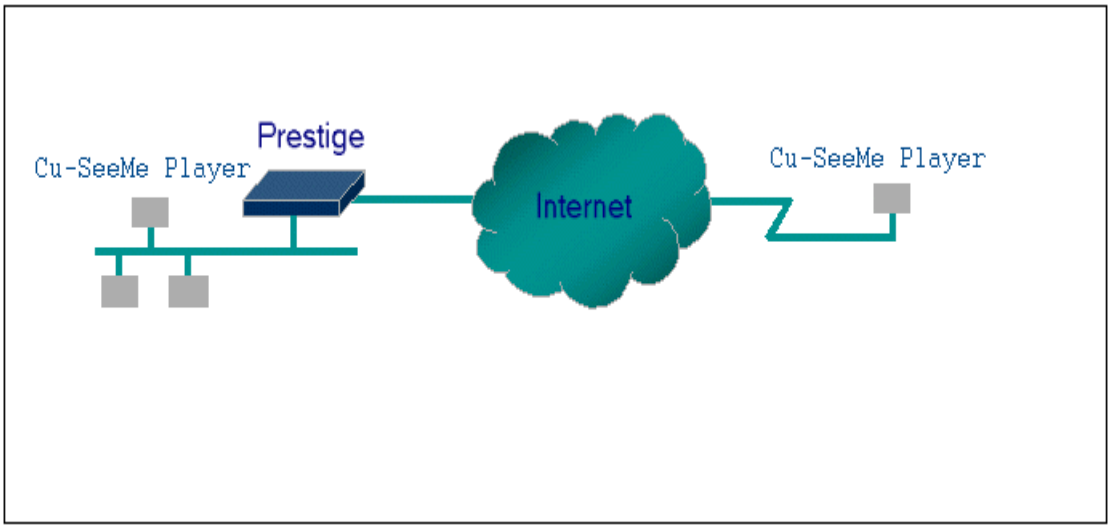
Ip dhcp enif0 mode relay

Ip dhcp enif0 relay server [Server IP Address]

8. SUA Notes

Tested SUA/NAT Applications (e.g., Cu-SeeMe, ICQ, NetMeeting)

All contents copyright © 2010 ZyXEL Communications Corporation.



Introduction

Generally, SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. However, some applications such as Cu-SeeMe, and ICQ will need to connect to the local user behind the P-793H v2. In such case, a SUA server must be configured to forward the incoming packets to the true destination behind SUA. After the required server are configured in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding,** the internal server or client applications can be accessed by using the P-793H v2's ***WAN IP* Address**.

SUA Supporting Table

The following are the required Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** for the various applications running SUA mode.

ZyXEL SUA Supporting Table[1]

Application	Required Settings in **Port Forwarding** Port/IP	
	Outgoing Connection	Incoming Connection
HTTP	None	80/client IP
FTP	None	21/client IP
TELNET	None	23/client IP (and active Telnet service from WAN)
POP3	None	110/client IP
SMTP	None	25/client IP
mIRC	None for Chat. For DCC, please set Default/Client IP	.
Windows PPTP	None	1723/client IP

All contents copyright © 2010 ZyXEL Communications Corporation.

ICQ 99a	None for Chat. For DCC, please set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
ICQ 2000b	None for Chat	None for Chat
ICQ Phone 2000b	None	6701/client IP
Cornell 1.1 Cu-SeeMe	None	7648/client IP
White Pine 3.1.2 Cu-SeeMe[2]	7648/client IP & 24032/client IP	Default/client IP
White Pine 4.0 Cu-SeeMe	7648/client IP & 24032/client IP	Default/client IP
Microsoft NetMeeting 2.1 & 3.01[3]	None	1720/client IP 1503/client IP
Cisco IP/TV 2.0.0	None	.
RealPlayer G2	None	.
VDOLive	None	.
Quake1.06[4]	None	Default/client IP
QuakeII2.30[5]	None	Default/client IP
QuakeIII1.05 beta	None	.
StartCraft.	6112/client IP	.
Quick Time 4.0	None	.
pcAnywhere 8.0	None	5631/client IP 5632/client IP 22/client IP
IPsec (ESP tunneling mode)	None (one client only)	Default/Client
Microsoft Messenger Service 3.0	6901/client IP	6901/client IP
Microsoft Messenger Service 4.6/ 4.7/ 5.0/… (none UPnP)[6]	None for Chat, File transfer ,Video and Voice	None for Chat, File transfer, Video and Voice
Net2Phone	None	6701/client IP
Network Time Protocol (NTP)	None	123 /server IP
Win2k Terminal Server	None	3389/server IP
Remote Anything	None	3996 - 4000/client IP
Virtual Network Computing	None	5500/client IP

All contents copyright © 2010 ZyXEL Communications Corporation.

(VNC)		5800/client IP 5900/client IP
AIM (AOL Instant Messenger)	None for Chat and IM	None for Chat and IM
e-Donkey	None	4661 - 4662/client IP
POLYCOM Video Conferencing	None	Default/client IP
iVISTA 4.1	None	80/server IP
Microsoft Xbox Live[7]	None	N/A

[1] Since SUA enables your LAN to appear as a single computer to the Internet, it is not possible to configure similar servers on the same LAN behind SUA.

[2] Because White Pine Cu-SeeMe uses dedicate ports (port 7648 & port 24032) to transmit and receive data, therefore only one local Cu-SeeMe is allowed within the same LAN.

[3] In SUA mode, only one local NetMeeting user is allowed because the outsiders can not distinguish between local users using the same internet IP.

[4] Certain Quake servers do not allow multiple users to login using the same unique IP, so only one Quake user will be allowed in this case. Moreover, when a Quake server is configured behind SUA, P-793H v2 will not be able to provide information of that server on the internet.

[5] Quake II has the same limitations as that of Quake I.

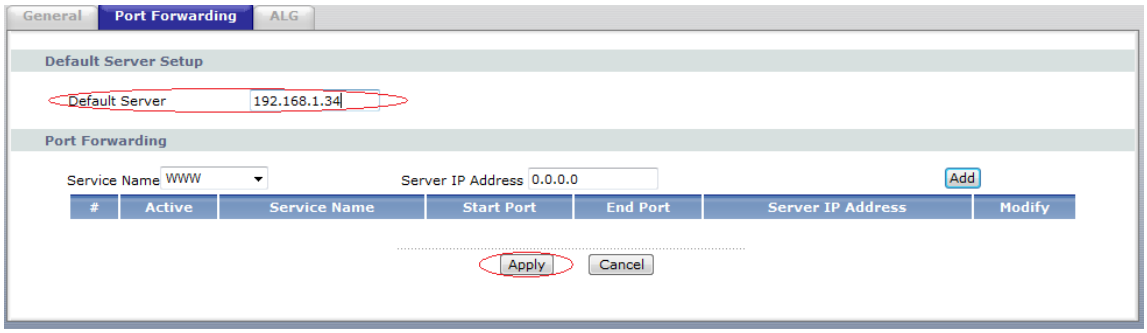
[6] P-793H v2 supports MSN Messenger 4.6/ 4.7/ 5.0/… video/ voice pass-through NAT. In addition, for the Windows OS supported UPnP (Universal Plug and Play), such as Windows XP and Windows ME, UPnP supported in P-793H v2 is an alternative solution to pass through MSN Messenger video/ voice traffic. For more detail, please refer to UPnP application note.

[7] P-793H v2 support Microsoft Xbox Live with factory default configuration.

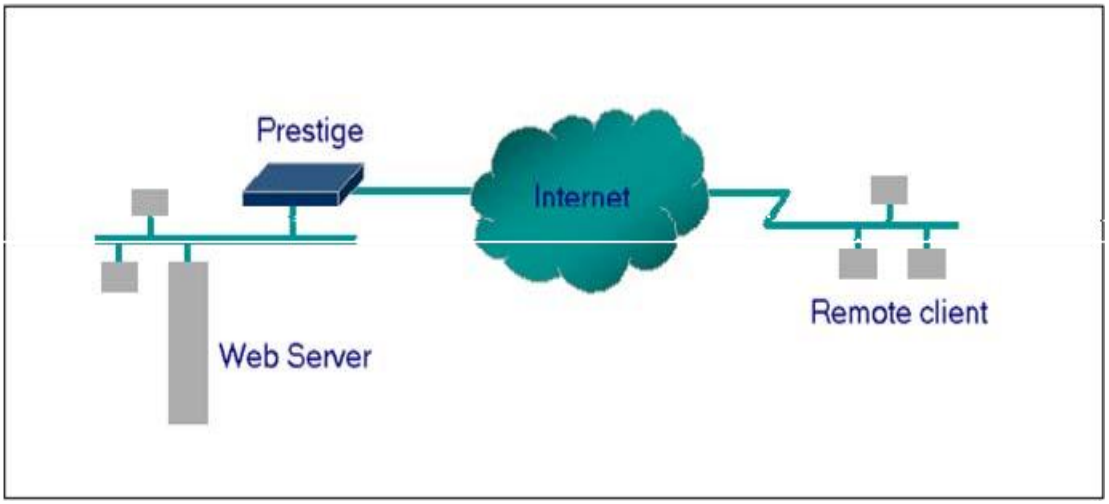
Configurations

For example, if the workstation operating Cu-SeeMe has an IP of 192.168.1.34, then the default SUA server must be set to 192.168.1.34. The peer Cu-SeeMe user can reach this workstation by using P-793H v2's ***WAN IP*** address which can be obtained from Web Configurator, **Status -> WAN Information**.

All contents copyright © 2010 ZyXEL Communications Corporation.



Configure an Internal Server behind SUA



Introduction

If you wish, you can make internal servers (e.g., Web, ftp or mail server) accessible for outside users, even though SUA makes your LAN appear as a single machine to the outside world. A service is identified by the port number. Also, since you need to specify the IP address of a server behind the P-793H v2, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time P-793H v2 is powered on.

In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server in Web Configurator, Advanced

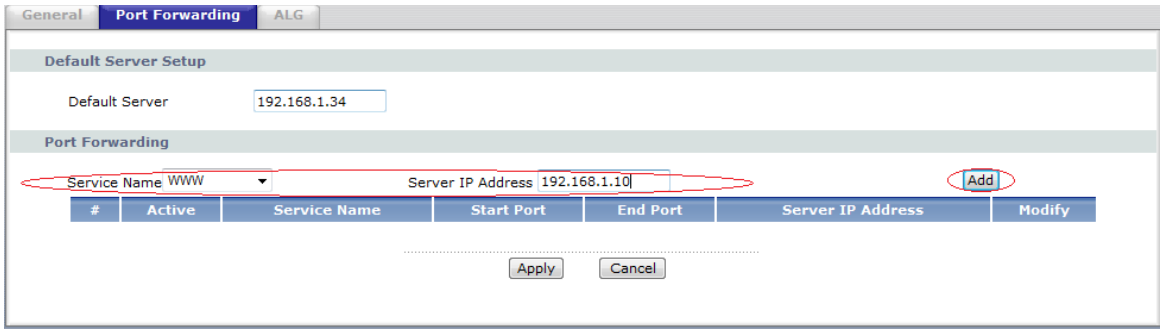
All contents copyright © 2010 ZyXEL Communications Corporation.

Setup, **Network -> NAT -> Port Forwarding.** The outside users can access the local server using the P-793H v2's ***WAN IP*** address which can be obtained from Web Configurator, **Status -> WAN Information**.

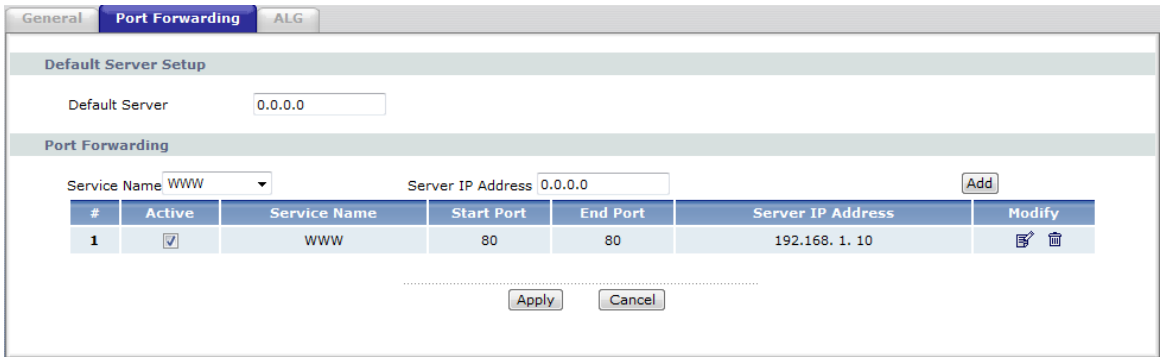
For example:

Configuring an internal Web server for outside access (suppose the Server IP Address is 192.168.1.10) :

(1) Fill in the service name and server IP Address, press button 'Add'



(2) If add successfully, the Web Configurator will display message 'Configuration updated successfully' at the bottom. You can see the port forwarding rule on the same page, the default port for Web Server is 80:



(3) If you want to change the port for Web Server, you could press button 'Modify' on corresponding rule, then modify and apply it.

Default port numbers for some services

Service	Port Number
FTP	21

All contents copyright © 2010 ZyXEL Communications Corporation.

Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80

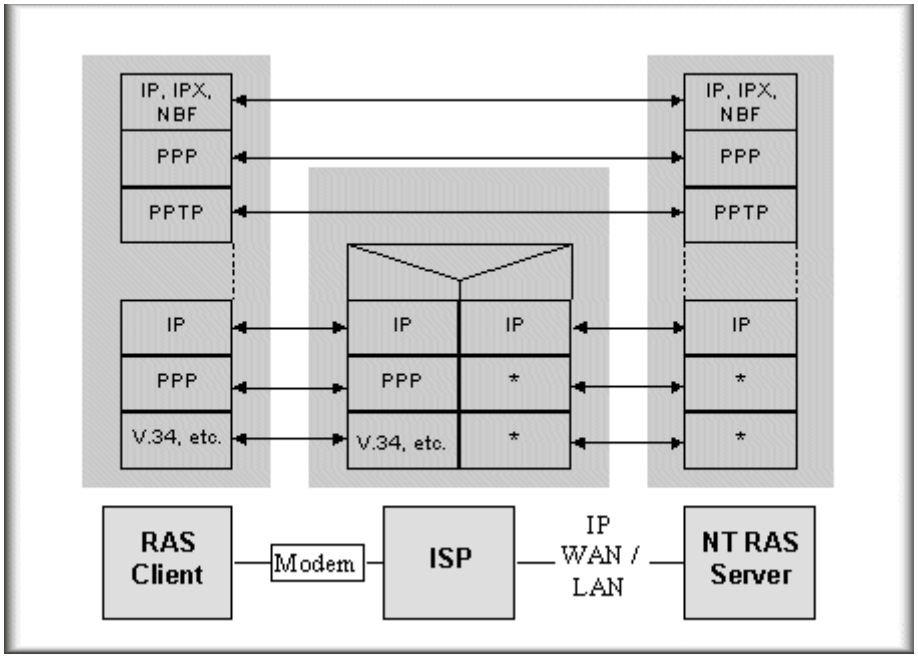
Configure a PPTP server behind SUA

Introduction

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself.

In order to run the Windows 9x PPTP client, you must be able to establish an IP connection with a tunnel server such as the Windows NT Server 4.0 Remote Access Server.

Windows Dial-Up Networking uses the Internet standard Point-to-Point (PPP) to provide a secure, optimized multiple-protocol network connection over dial-up telephone lines. All data sent over this connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, NetBEUI and IPX) can be run correctly. Windows NT Domain Login level security is preserved even across the Internet.

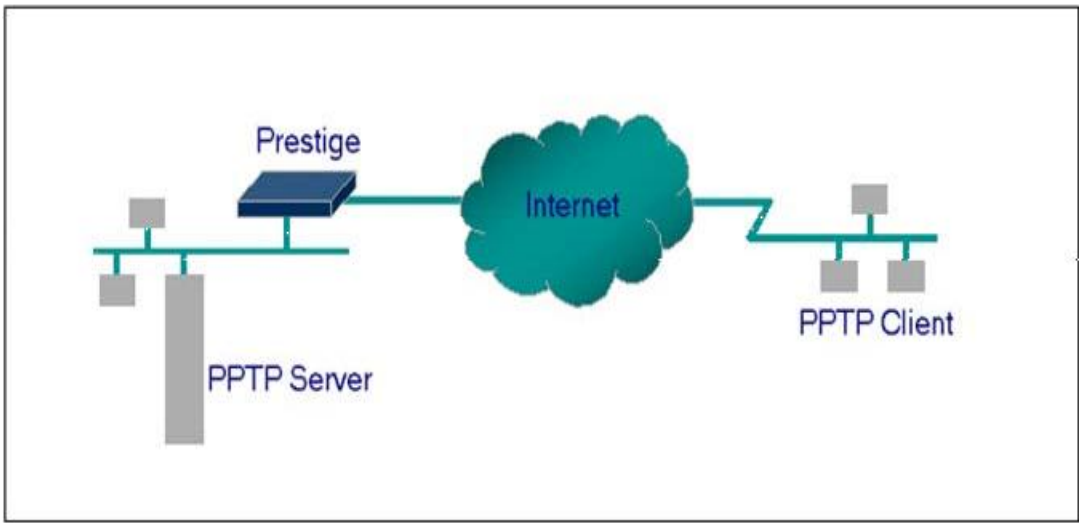


Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

All contents copyright © 2010 ZyXEL Communications Corporation.

PPTP appears as new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the Dial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial-up adapter that provides PPP support for the analog or ISDN modem.

The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.
This application note explains how to establish a PPTP connection with a remote private network in the P-793H v2 SUA case. In ZyNOS, all PPTP packets can be forwarded to the internal PPTP Server (WinNT server) behind SUA. The port number of the PPTP has to be entered in the Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** on P-793H v2 to forward to the appropriate private IP address of Windows NT server.



Example

The following example shows how to dial to an ISP via the P-793H v2 and then establish a tunnel to a private network. There will be three items that you need to set up for PPTP application, these are PPTP server (WinNT), PPTP client (Win9x) and the P-793H v2.

(1) PPTP server setup (WinNT)

- Add the VPN service from Control Panel ->Network

All contents copyright © 2010 ZyXEL Communications Corporation.

- Add an user account for PPTP logged on user
- Enable RAS port
- Select the network protocols from RAS such as IPX, TCP/IP NetBEUI
- Set the Internet gateway to P-793H v2

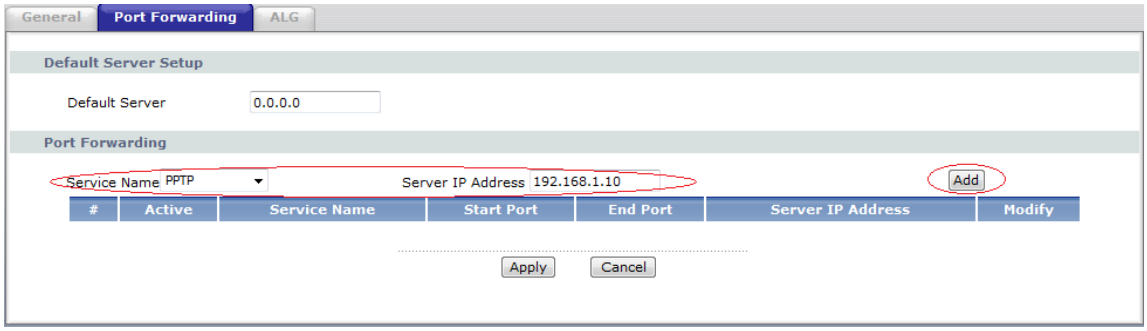
(2) PPTP client setup (Win9x)

- Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the P-793H v2's Internet IP address for logging to NT RAS server.
- Set the Internet gateway to the router that is connecting to ISP

(3) P-793H v2 setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect P-793H v2 router to your ISP first.
- Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown below:

Select service name as 'PPTP', fill in the Server IP Address, then press button 'Add'.



When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the Internet. If the Internet connection between two LANs is achievable, you can place a VPN call from the remote Win9x client.

For example: C:\ping 203.66.113.2

When a dial-up connection to ISP is established, a default gateway is assigned to the router traffic through that connection. Therefore, the output below shows the default gateway of the Win9x client after the dial-up connection has been established.

All contents copyright © 2010 ZyXEL Communications Corporation.

Before making a VPN connection from the Win9x client to the NT server, you need to know the exact Internet IP address that the ISP assigns to P-793H v2 router in SUA mode and enter this IP address in the VPN dial-up dialog box.

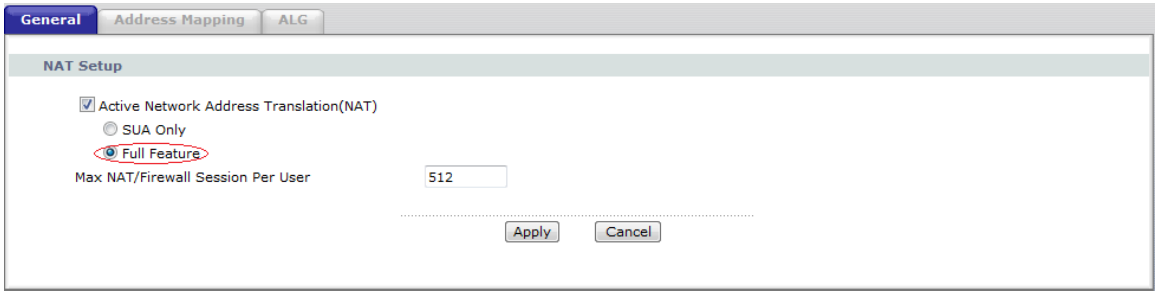
You can check this Internet IP address from PNC Monitor or Web Configurator, **Status -> WAN Information**.

If the Internet IP address is a fixed IP address provided by ISP in SUA mode, then you can always use this IP address for reaching the VPN server.

In the following example, the IP address '140.113.1.225' is dynamically assigned by ISP. You must enter this IP address in the 'VPN Server' dialog box for reaching the PPTP server. After the VPN link is established, you can start the network protocol application such as IP, IPX and NetBEUI.

9. Using Full Feature NAT

When P-793H v2 is in Routing mode, you can select NAT Option as Full Feature in Network -> NAT -> Genaral:



Key Settings:

Field	Options	Description
Network Address Translation	**Full Feature**	When you select this option you can select Address Mapping Set Number 1~8 in the pull-down menu on the right.

All contents copyright © 2010 ZyXEL Communications Corporation.

	None	NAT is disabled when you select this option.
	SUA Only	When you select this option, this remote node will use default SUA Address Mapping Set. You can see it in CLI by command '**ip nat lookup 255**'. It's a read-only sets with two rules: **Many-to-One** and **server** mapping. Select **Full Feature** when you require other mapping types.

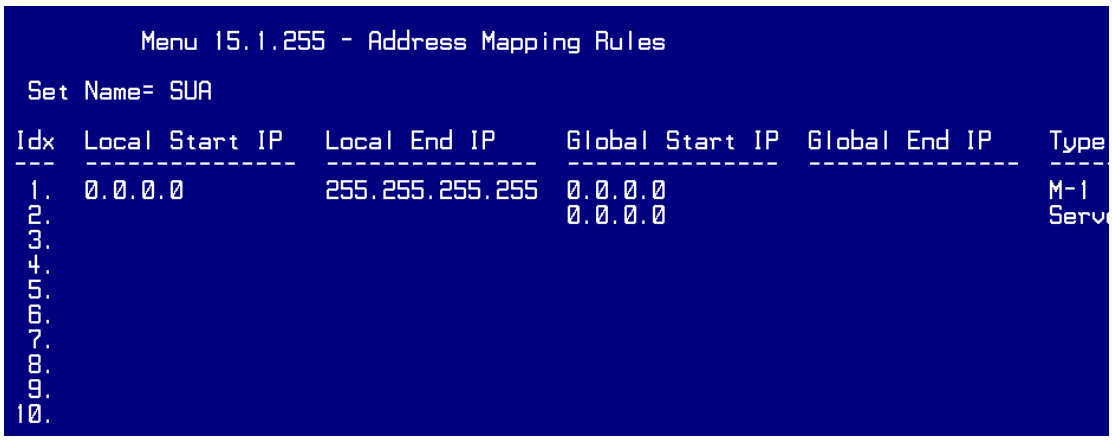
Configuring NAT

The P-793H v2 has 8 remote nodes and so allows you to configure 8 NAT Address Mapping Sets, You must specify which NAT Address Mapping Set (1~8) to use in the remote node when you select **Full Feature NAT.**

You can edit 10 rules for each Address Mapping Set. You can edit the rules for Address Mapping Sets #1 in Web Configurator. The other Address Mapping Sets #2~8 can only be configured in CLI (Command Line Interface).

The NAT Server Set is a list of LAN side servers mapped to external ports. We can configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding.** To use the NAT server sets you've configured, a **Server** rule must be set up inside the NAT Address Mapping set. Please see NAT Server Sets for further information on how to apply it.

When you select **SUA Only,** the P-793H v2 will use a default SUA Address Mapping set for it. It has two rules: **Many-to-One** and **Server**. You can see it in SMT menu 15.



Please note that the fields in this menu are read-only. However, the settings of the rule set 2 can be modified in Web Configurator, Advanced Setup, **Network**

All contents copyright © 2010 ZyXEL Communications Corporation.

-> NAT -> Port Forwarding. The following table explains the fields in this above screen:

Field	Description	Option/Example
set	This is sequence number for Address Mapping Sets	255 for SUA
Internal Start IP	This is the starting local IP address (ILA).	0.0.0.0 for the Many-to-One type.
Local End IP	This is the starting local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	N/A

NAT Server Sets

The NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu of before). If you wish, you can make inside servers for different services, e.g., Web or FTP, visible to the outside users, even though NAT makes your network appears as a single machine to the outside world. A server is identified by the port number, e.g., Web service is on port 80 and FTP on port 21.

As an example (see the following figure), if you have a Web server at 192.168.1.36 and a FTP server at 192.168.1.33, then you need to specify for port 80 (Web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.

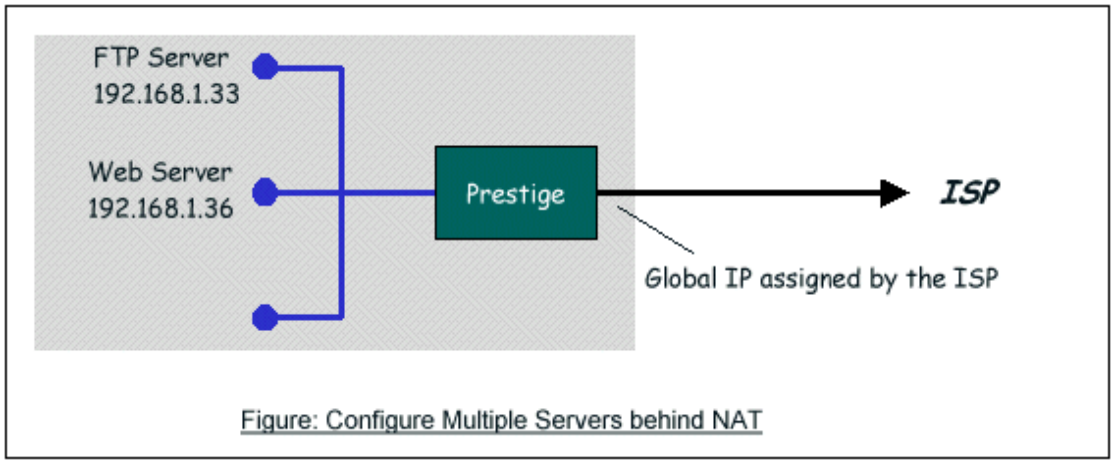


Figure: Configure Multiple Servers behind NAT

All contents copyright © 2010 ZyXEL Communications Corporation.

Please note that a server can support more than one service, e.g., a server can provide both FTP and Mail service, while another provides only Web service.
The following procedures show how to configure a server behind NAT.
Step 1: Login Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding.**
Step 2: Select the service name from the pull-down menu, and fill in the server Address on '**Server IP Address**', then click button '**Add**' to save it.
Step 3: You could click the button 'Edit' on the rule to modify the Service name, Server IP Address, Start/End Port.

The most often used port numbers are shown in the following table. Please refer RFC 1700 for further information about port numbers.

Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

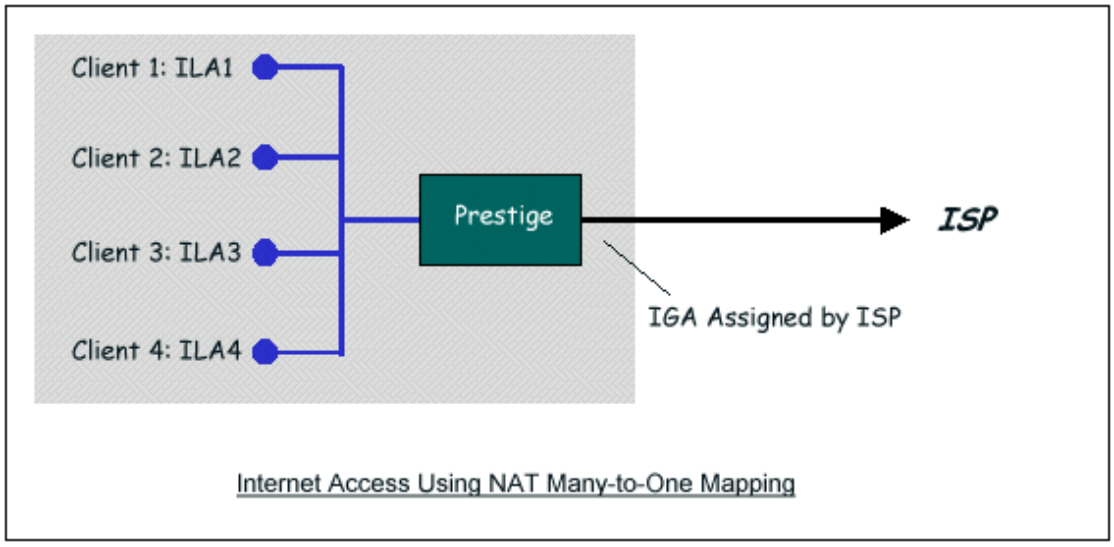
Examples

- Internet Access Only
- Internet Access with an Internal Server
- Using Multiple Global IP addresses for clients and servers
- Support Non NAT Friendly Applications

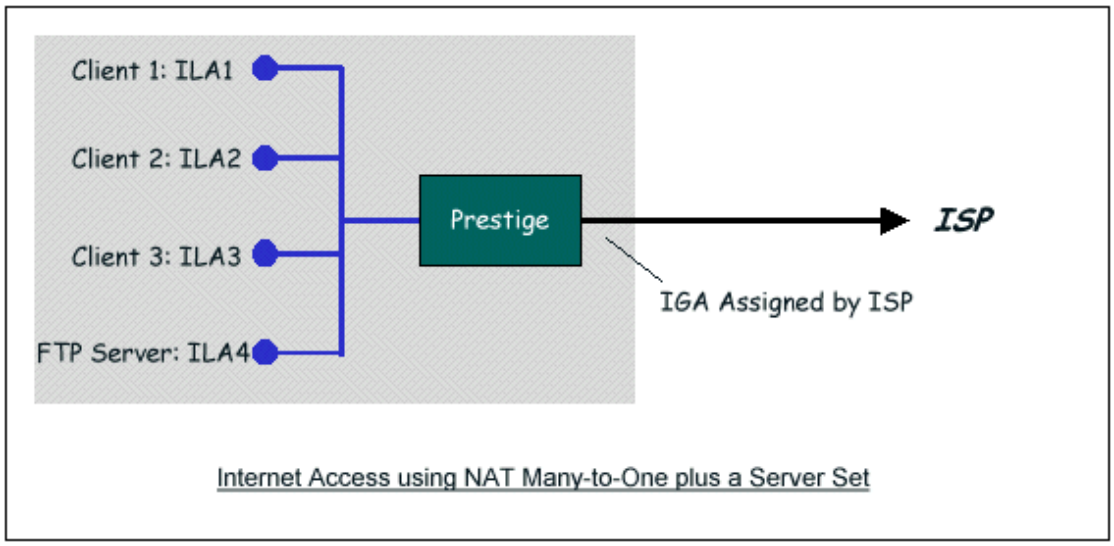
(1) Internet Access Only

In our Internet Access example, we only need one rule where all our ILAs map to one IGA assigned by the ISP. You can just use the default **SUA NAT**, or you could select **Full Feature NAT** and select an Address Mapping Set with a **Many-to-One** Rule. See the following figure.

All contents copyright © 2010 ZyXEL Communications Corporation.



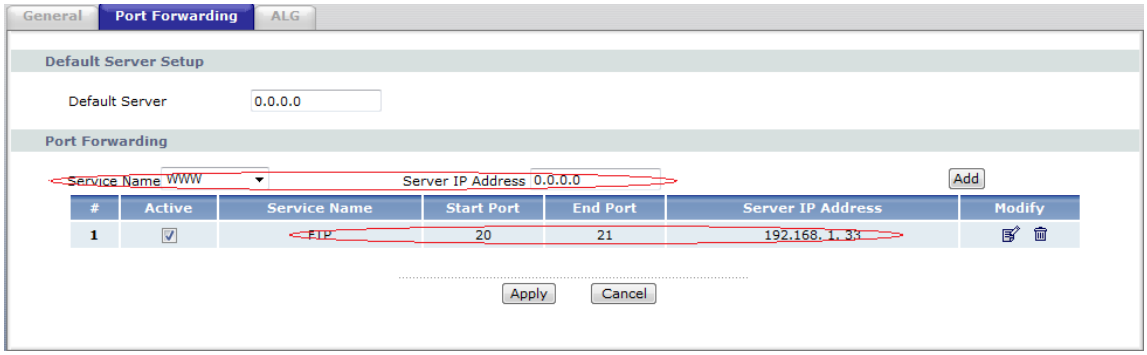
(2) Internet Access with an Internal Server



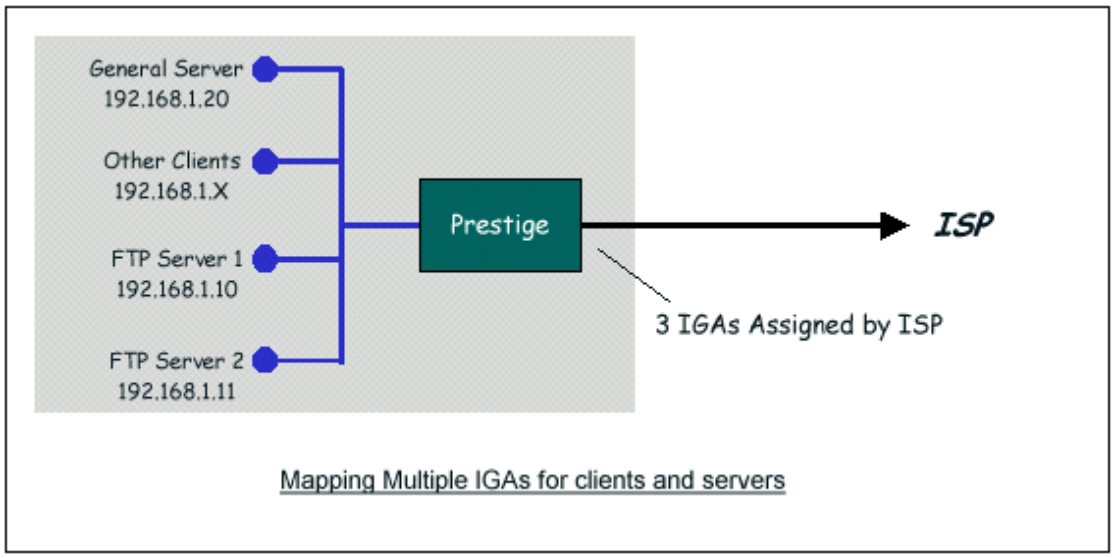
In this case, we do exactly as the figure (use the convenient pre-configured SUA Only set) and also go to Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** to specify the Internet Server behind the NAT as

All contents copyright © 2010 ZyXEL Communications Corporation.

below:



(3) Using Multiple Global IP addresses for clients and servers (One-to-One, Many-to-One, Server Set mapping types are used)



In this case we have 3 IGAs from the ISP. We have two very busy internal FTP servers and also an internal general server for the web and mail. In this case, we want to assign the 3 IGAs by the following way using 4 NAT rules.

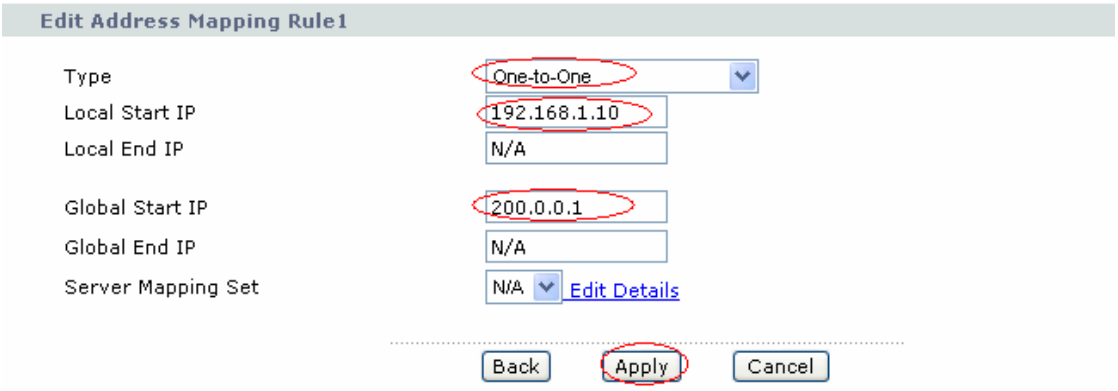
- Rule 1 (One-to-One type) to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).
- Rule 2 (One-to-One type) to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).
- Rule 3 (Many-to-One type) to map the other clients to IGA3 (200.0.0.3).
- Rule 4 (Server type) to map a web server and mail server with ILA3 (192.168.1.20) to IGA3. Type **Server** allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

All contents copyright © 2010 ZyXEL Communications Corporation.

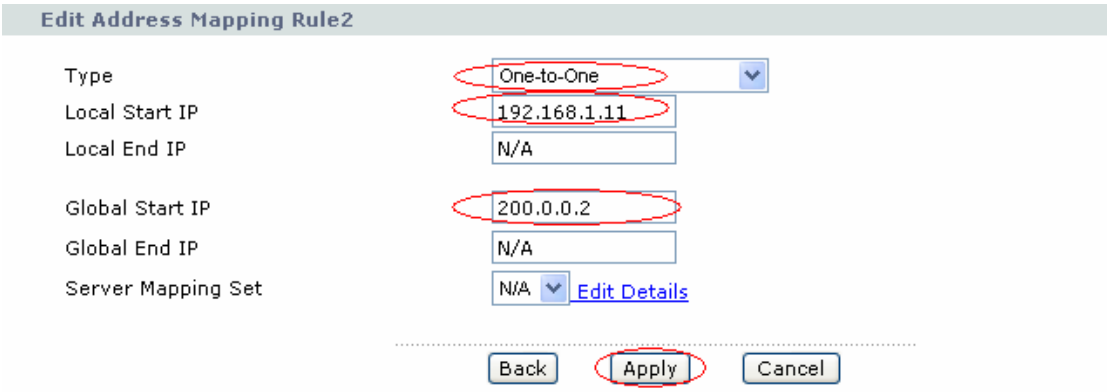
Step 1: In this case, we need to map ILA to more than one IGA, therefore we must choose the **Full Feature** option from the **NAT** field in currently active remote node, and assign IGA3 to P-793H v2's WAN IP Address.

Step 2: Go to Web Configurator, Advanced Setup, **Network -> NAT -> Address Mapping** to begin configuring Address Mapping Set #1. We can see there are 10 blank rule table that could be configured. See the following setup for the four rules in our case.

Rule 1 Setup: Select **One-to-One** type to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).

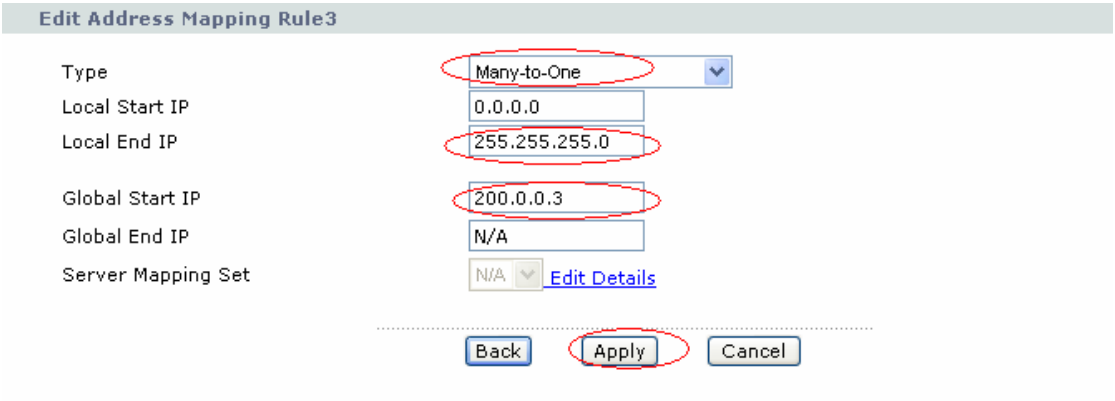


Rule 2 Setup: Selecting **One-to-One** type to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).

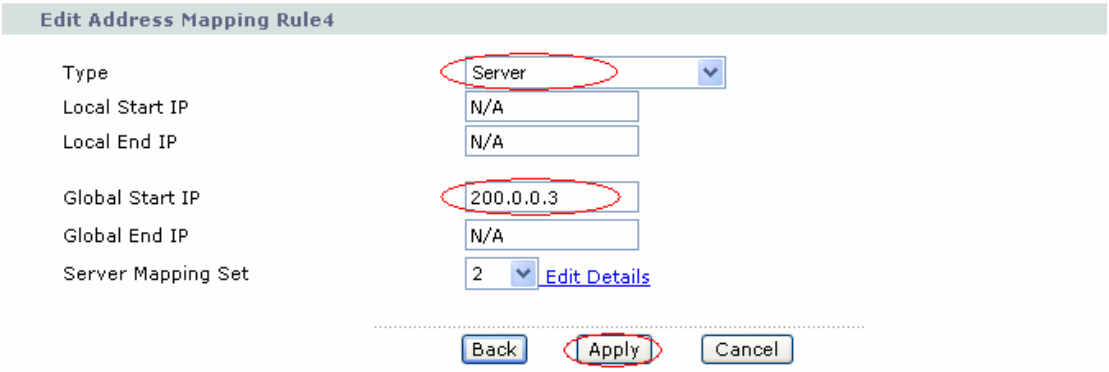


Rule 3 Setup: Select **Many-to-One** type to map the other clients to IGA3 (200.0.0.3).

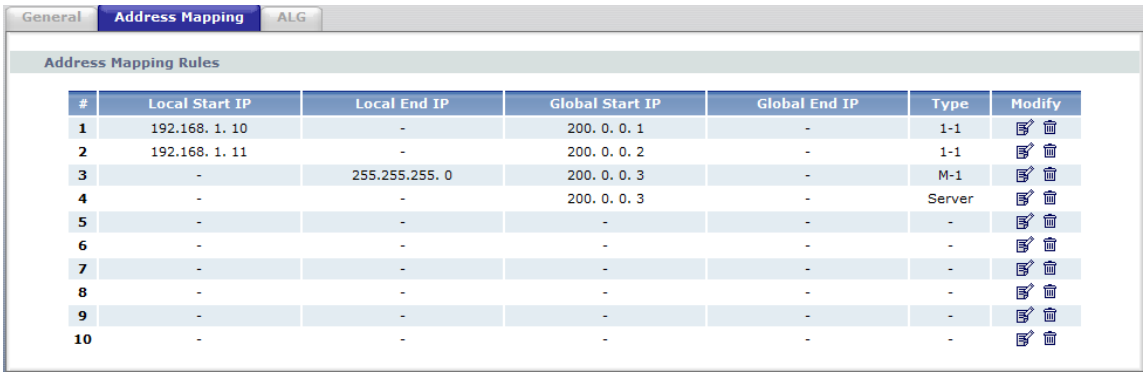
All contents copyright © 2010 ZyXEL Communications Corporation.



Rule 4 Setup: Select **Server type** to map our web server and mail server with ILA3 (192.168.1.20) to IGA3.



Menu **Network -> NAT -> Address Mapping** should look as follows now:



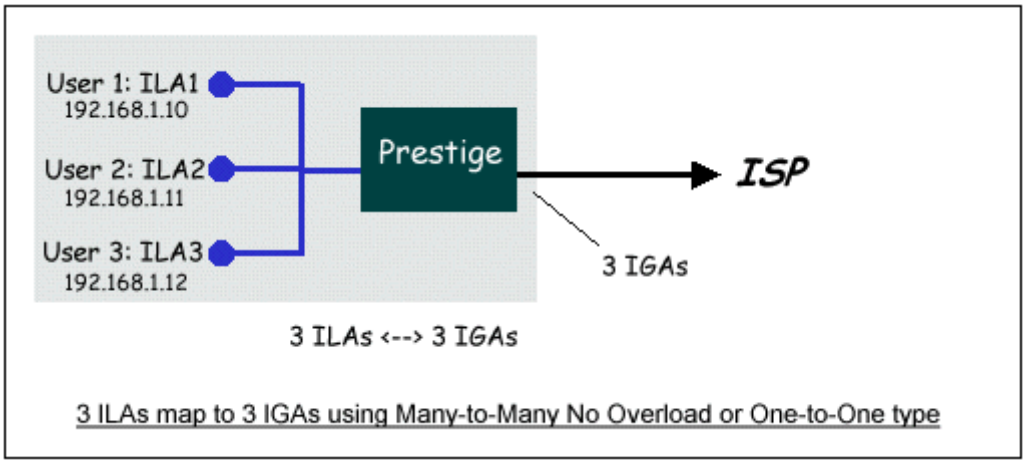
#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168. 1. 10	-	200. 0. 0. 1	-	1-1	
2	192.168. 1. 11	-	200. 0. 0. 2	-	1-1	
3	-	255.255.255. 0	200. 0. 0. 3	-	M-1	
4	-	-	200. 0. 0. 3	-	Server	
5	-	-	-	-	-	
6	-	-	-	-	-	
7	-	-	-	-	-	
8	-	-	-	-	-	
9	-	-	-	-	-	
10	-	-	-	-	-	

Step 3: Now we configure all other incoming traffic to go to our web server and mail server from Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding:**

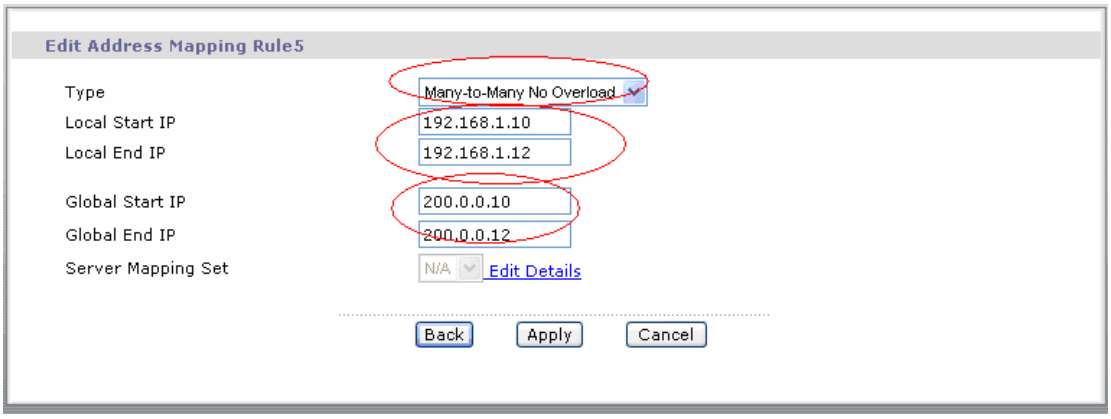
(4) Support Non NAT Friendly Applications

All contents copyright © 2010 ZyXEL Communications Corporation.

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user login to the server using a unique global IP address. The following figure illustrates this.



One rule configured for using **Many-to-Many No Overload** mapping type is shown below.



We can also do this by configure three**One-to-One** mapping type rules.

10. Using the Dynamic DNS (DDNS)

- What is DDNS?

The DDNS service, an IP Registry provides a public central database where information such as email addresses, hostnames, IPs etc. can be stored and retrieved. This solves the problems if your DNS server uses an IP associated with dynamic IPs.

Without DDNS, we always tell the users to use the WAN IP of the P-793H v2 to access the internal server. It is inconvenient for the users if this IP is dynamic.

All contents copyright © 2010 ZyXEL Communications Corporation.

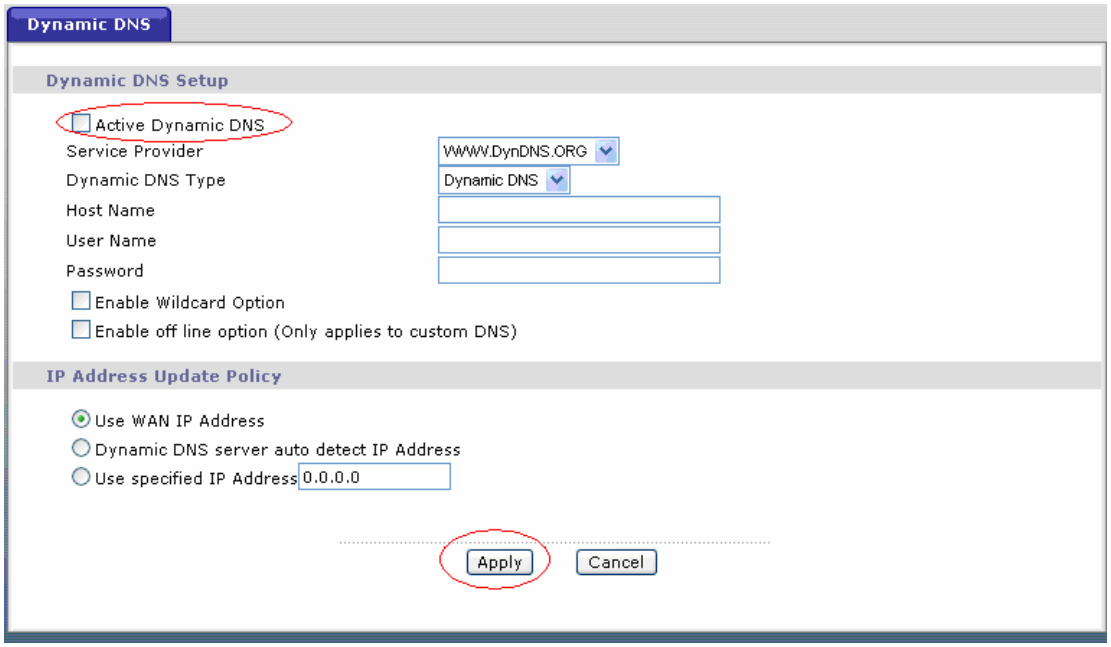
With DDNS supported by the P-793H v2, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-793H v2.

When the ISP assigns the P-793H v2 a new IP, the P-793H v2 must inform the DDNS server the change of this IP so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

The DDNS servers the P-793H v2supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

- Setup the DDNS

1. Before configuring the DDNS settings in the P-793H v2, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you have a hostname for your internal server and a password using to update the IP to the DDNS server.
2. Login Web Configurator, Advanced Setup, **Advanced -> Dynamic DNS** Select **'Active Dynamic DNS'** option:



Key Settings:

Option	Description
Service Provider	Enter the DDNS server in this field. Currently, we support WWW.DYNDNS.ORG.

All contents copyright © 2010 ZyXEL Communications Corporation.

Active	Toggle to **'Yes'**.
Host Name	Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw.
User Name	Enter the user name that the DDNS server gives to you.
Password	Enter the password that the DDNS server gives to you.
Enable Wildcard	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is http://www.dyndns.org/.

11. Network Management Using SNMP

- ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some P-793H v2 routers. It is implemented based on the SNMP v1, so it will be able to communicate with SNMPv1 NMSs. Further, users can also add ZyXEL's private MIB in the NMS to monitor and control additional system variables. The ZyXEL's private MIB tree is shown in figure 3. For SNMP v1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

Some traps are sent to the SNMP manager when anyone of the following events happens:

1. coldStart (defined in RFC-1215) :

   If the machine coldstarts, the trap will be sent after booting.

2. warmStart (defined in RFC-1215) :

   If the machine warmstarts, the trap will be sent after booting.

3. linkDown (defined in RFC-1215) :

   If any link of IDSL or WAN is down, the trap will be sent with the port number. The port number is its interface index under the interface group.

4. linkUp (defined in RFC-1215) :

   If any link of IDSL or WAN is up, the trap will be sent with the port number. The port number is its interface index under the interface group.

All contents copyright © 2010 ZyXEL Communications Corporation.

5. authentication Failure (defined in RFC-1215) :

When receiving any SNMP get or set requirement with wrong community, this trap is sent to the manager.

6. why Reboot (defined in ZYXEL-MIB) :

When the system is going to restart (warm start), the trap will be sent with the reason of restart before rebooting.

(1) For intentional reboot :
In some cases (download new files, CI command "sys reboot"), reboot is done intentionally. And traps with the message "System reboot by user !" will be sent.

(2) For fatal error :
System has to reboot for some fatal errors. And traps with the message of the fatal code will be sent.

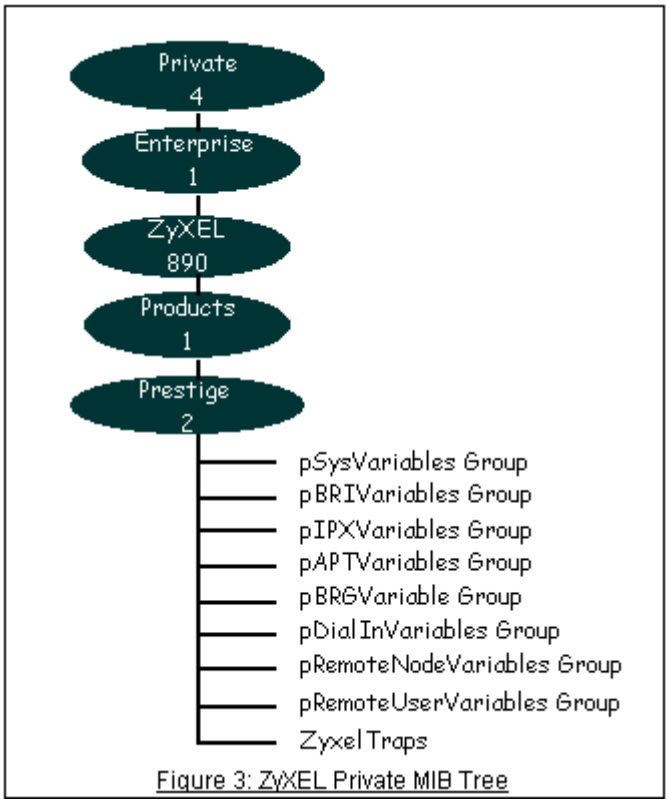
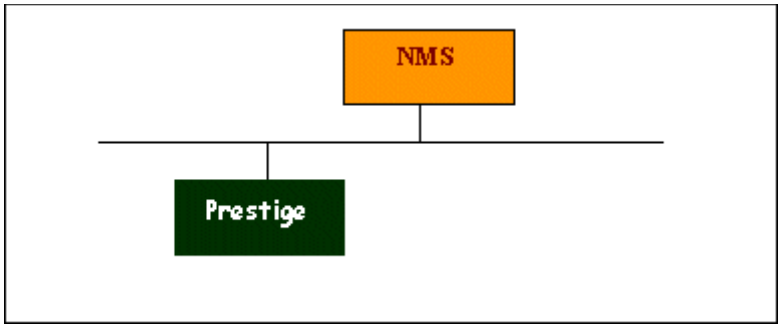


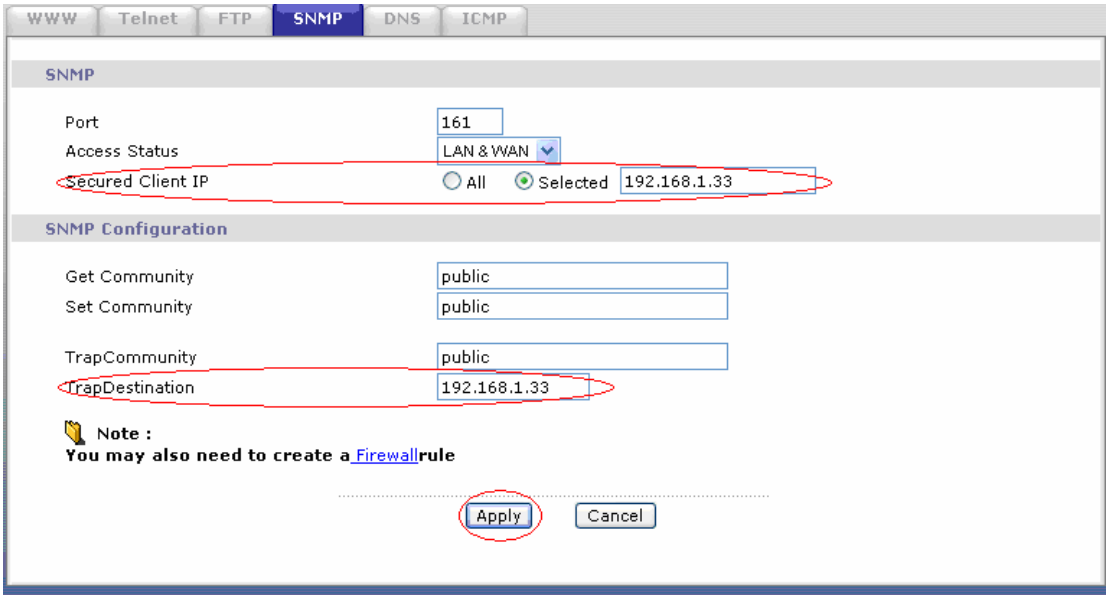
Figure 3: ZyXEL Private MIB Tree

- Configure the P-793H v2 for SNMP

All contents copyright © 2010 ZyXEL Communications Corporation.



The SNMP related settings in P-793H v2are configured in Web Configurator, Advanced Setup, **Advanced -> Remote MGNT -> SNMP** The following steps describe a simple setup procedure for configuring all SNMP settings.



Key Settings:

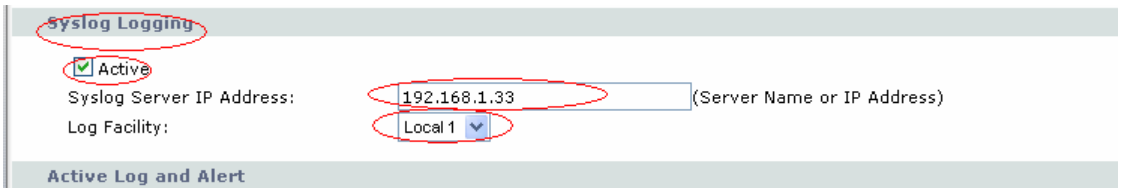
Option	Descriptions
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
Trusted Host	Enter the IP address of the NMS. The P-793H v2w ill only respond to SNMP messages coming from this IP address. **If 0.0.0.0 is entered, the P-793H v2 will respond to all NMS managers.**
Trap Community	Enter the community name in each sent trap to the NMS. This Trap Community must match w hat the NMS is expecting. The default is 'public'.

All contents copy right © 2010 Zy XEL Communications Corporation.

Trap Destination	Enter the IP address of the NMS that you wish to send the traps to. **If 0.0.0.0 is entered, the P-793H v2 will not send trap any NMS manager.**

Note: You may need to edit a firewall rule to permit SNMP Packets.

12. Using syslog



You can configure it in Web Configurator, Advanced Setup, **Maintenance -> Logs -> Log Settings -> Syslog logging.**

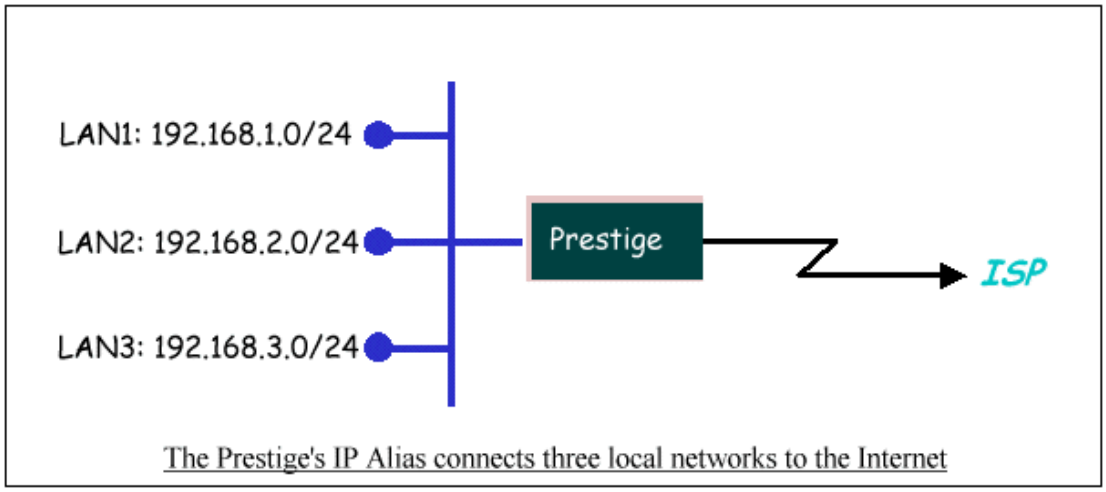
Key Settings:
Active: Select it to active UNIX Syslog.
Syslog IP Address: Enter the IP address of the UNIX server that you wish to send the syslog.
Log Facility: Select from the 7 different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.

13. Using IP Alias

- **What is IP Alias?**

In a typical environment, a LAN router is required to connect two local networks. The P-793H v2can connect three local networks to the ISP or a remote node, we call this function as **'IP Alias'**. In this case, an internal router is not required. For example, the network manager can divide the local network into three networks and connect them to the Internet using P-793H v2's single user account. See the figure below.

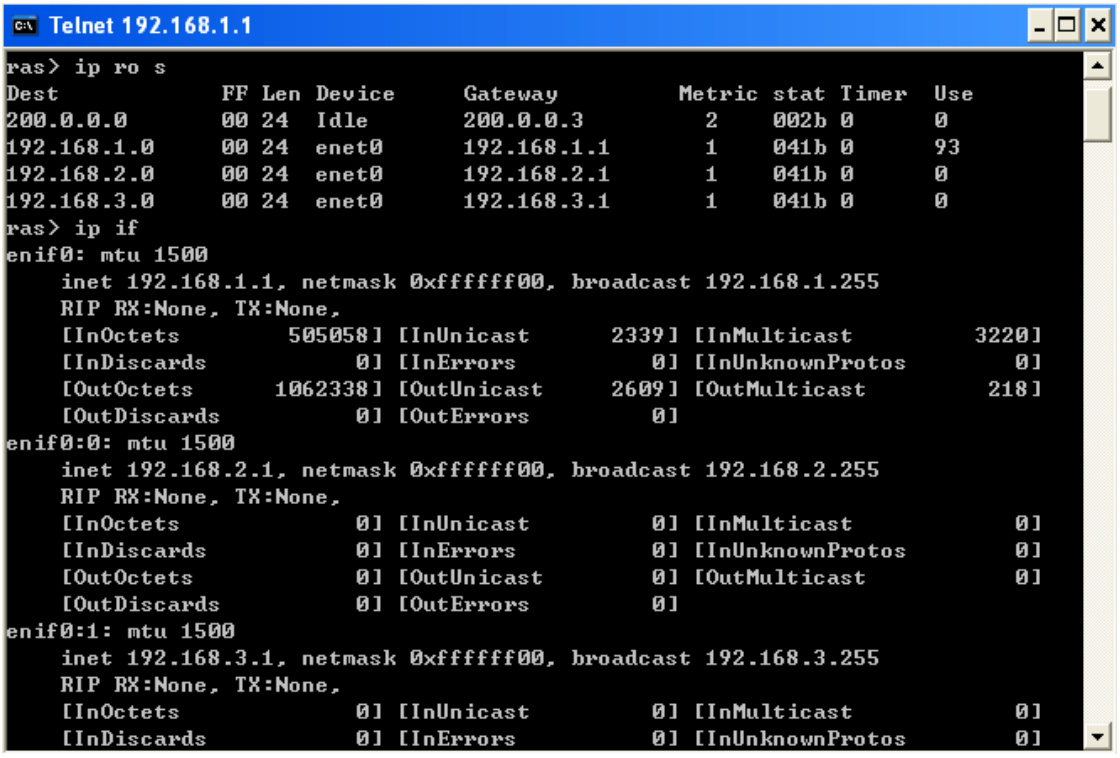
All contents copyright © 2010 ZyXEL Communications Corporation.



The Prestige's IP Alias connects three local networks to the Internet

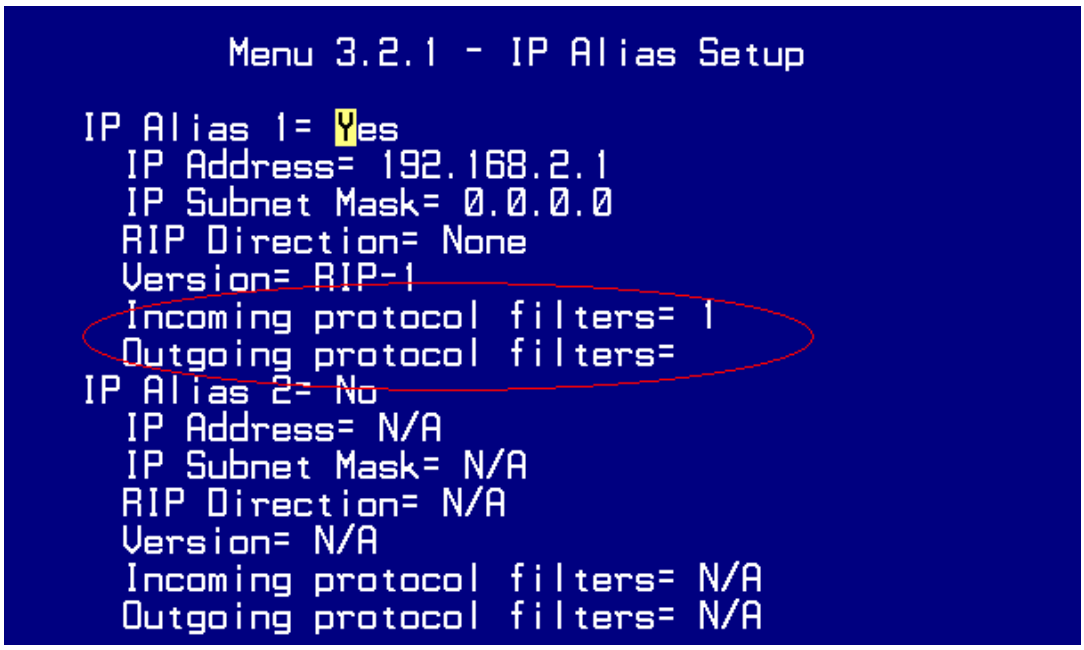
The P-793H v2supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured in Web Configurator, Advanced Setup, **Network -> LAN -> DHCP Setup**. The second and third networks that we call **'IP Alias 1'** and **'IP Alias 2'** can be configured in **Network -> LAN -> IP Alias**.

There are three internal virtual LAN interfaces for the P-793H v2 to route the packets from/to the three networks correctly. They are **enif0** for the major network, **enif0:0** for the IP alias 1 and **enif0:1** for the IP alias 2. Therefore, three routes are created in the P-793H v2 as shown below when the three networks are configured. If the P-793H v2's DHCP is also enabled, the IP pool for the clients can be any of the three networks.


Telnet 192.168.1.1
ras> ip ro s
Dest FF Len Device Gateway Metric stat Timer Use
200.0.0.0 00 24 Idle 200.0.0.3 2 002b 0 0
192.168.1.0 00 24 enet0 192.168.1.1 1 041b 0 93
192.168.2.0 00 24 enet0 192.168.2.1 1 041b 0 0
192.168.3.0 00 24 enet0 192.168.3.1 1 041b 0 0
ras> ip if
enif0: mtu 1500
inet 192.168.1.1, netmask 0xffffff00, broadcast 192.168.1.255
RIP RX:None, TX:None,
[InOctets 505058] [InUnicast 2339] [InMulticast 3220]
[InDiscards 0] [InErrors 0] [InUnknownProtos 0]
[OutOctets 1062338] [OutUnicast 2609] [OutMulticast 218]
[OutDiscards 0] [OutErrors 0]
enif0:0: mtu 1500
inet 192.168.2.1, netmask 0xffffff00, broadcast 192.168.2.255
RIP RX:None, TX:None,
[InOctets 0] [InUnicast 0] [InMulticast 0]
[InDiscards 0] [InErrors 0] [InUnknownProtos 0]
[OutOctets 0] [OutUnicast 0] [OutMulticast 0]
[OutDiscards 0] [OutErrors 0]
enif0:1: mtu 1500
inet 192.168.3.1, netmask 0xffffff00, broadcast 192.168.3.255
RIP RX:None, TX:None,
[InOctets 0] [InUnicast 0] [InMulticast 0]
[InDiscards 0] [InErrors 0] [InUnknownProtos 0]

All contents copyright © 2010 ZyXEL Communications Corporation.

You can edit filter rule to accept or deny LAN packets from/to the IP alias 1/2 go through the P-793H v2 in SMT menu 3.2.1 as below:



b

Or by commands in **CLI**:

lan index [index number]

Usage: index number =1 main LAN
2 IP Alias#1
3 IP Alias#2

lan filter <incoming|outgoing> <tcpip|generic> [set#]

Usage: set#= the corresponding filter set number you've configured

lan save

- IP Alias Setup

(1) Edit the first network in Web Configurator, Advanced Setup, **Network -> LAN -> IP/DHCP Setup** by configuring the P-793H v2's first LAN IP address.

Key Settings:

DHCP Setup	If the P-793H v2's DHCP server is enabled, the IP pool for the clients can be any of the three networks.
TCP/IP Setup	Enter the first LAN IP address for the P-793H v2. This will create the first route

(2) Edit the second and third networks in **Network -> LAN -> IP Alias** by configuring the P-793H v2's second and third LAN IP addresses.

Key Settings:

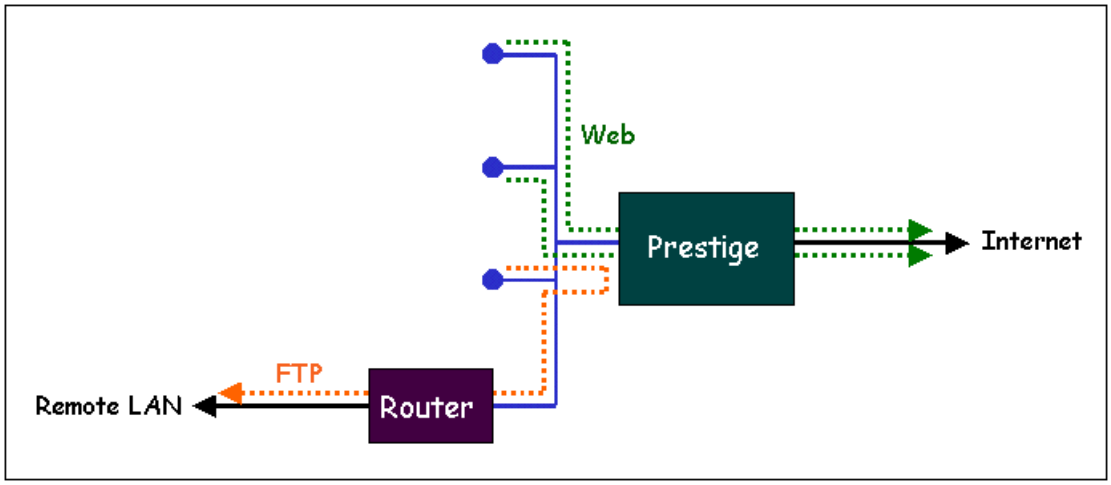
All contents copyright © 2010 ZyXEL Communications Corporation.

IP Alias 1	Active it and enter the second LAN IP address for the P-793H v2. This will create the second route in the enif0:0 interface.
IP Alias 2	Active it and enter the third LAN IP address for the P-793H v2. This will create the third route in the enif0:1 interface.

14. Using IP Policy Routing

- What is IP Policy Routing (IPPR)?

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Network administrators can use IPPR to distribute traffic among multiple paths. For example, if a network has both the Internet and remote node connections, we can route the Web packets to the Internet using one policy and route the FTP packets to the remote LAN using another policy. See the figure below.



Use IPPR to distribute traffic among multiple paths

- Benefits

Source-Based Routing - Network administrators can use policy-based routing to direct traffic from different users through different connections.

Quality of Service (QoS)- Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

All contents copyright © 2010 ZyXEL Communications Corporation.

Cost Savings- IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost path while using low-path for batch traffic.

Load Sharing- Network administrators can use IPPR to distribute traffic among multiple paths.

- How does the IPPR work?

A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP,etc), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., Telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the TOS and precedence fields in the IP header. IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A use defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

- Setup the IP Policy Routing

Rules can be edited in SMT menu 25.

Suppose we'd like to edit the rule like this:

```
Policy Set Name=Test
Active= Yes
 Criteria:
 IP Protocol    = 6
 Type of Service= Don't Care        Packet length= 0
 Precedence     = Don't Care         Len Comp= N/A
 Source:
   addr start= 192.168.1.2         end= 192.168.1.20
   port start= 0                  end= N/A
 Destination:
   addr start= 0.0.0.0             end= N/A
   port start= 80                 end= 80
Action= Matched
 Gateway addr   = 192.168.1.254      Log= No
```


All contents copyright © 2010 ZyXEL Communications Corporation.

Type of Service= No Change
Precedence = No Change

This policy example forces the Web packets originated from the clients with IP addresses from 192.168.1.2 to 192.168.1.20 be routed to the remote LAN via the gateway 192.168.1.254.

15. Using Call Scheduling

- What is Call Scheduling?

Call scheduling enables the mechanism for the P-793H v2 to run the remote node connection according to the pre-defined schedule. This feature is just like the scheduler in a video recorder which records the program according to the specified time. Users can apply at most 4 schedule sets in Remote Node. The remote node configured with the schedule set could be "Forced On", "Forced Down", "Enable Dial-On-Demand", or "Disable Dial-On-Demand" on specified date and time.

- How to configure a Call Scheduling?

You can configure a call scheduling in SMT menu 26.

Suppose we want to edit a call schedule set like this:

Call Schedule Set #=1
Set name=Test
Active= Yes
Start Date(yyyy-mm-dd)= 2005 - 12 - 27
How Often= Once
Once:
Date(yyyy-mm-dd)= 2005 -12 -27
Start Time(hh:mm)= 12 : 00
Duration(hh:mm)= 16 : 00
Action= Enable Dial-on-demand

This schedule example permits a demand call on the line on 12:00 a.m., 2005-12-27. The maximum length of time this connection is allowed is 16 hours.

Key Settings:

All contents copyright © 2010 ZyXEL Communications Corporation.

Start Date	Start date of this schedule rule. It can be unmatched with weekday setting. For example, if Start Date is 2000/10/02(Monday), but Monday setting in weekday can be No.
Forced On	The node will always keep up during the setting period. It is equivalent to disable the idle timeout.
Forced Down	The node will always keep open during the setting period. The connected remote node will be dropped.
Enable Dial-On-Demand	The remote node accepts Dial-on-demand during this period.
Disable Dial-On-Demand	The remote node denies any demand dial during the period. For the existing connected nodes, it will be dropped after idle timeout and no triggered up.
Start Time/ Duration	Start Time and Duration of this schedule.

- Apply the schedule to the Remote node

Multiple scheduling rules can program in a Remote node, and they have priority. For example, if we program the sets as 1,2,3,4 in remote node, then the set 1 will override set 2,3,4. set 2 will override 3,4, and so on.
We can apply the schedule to the remote node in SMT menu 11.1.
For example, if we want to apply the call schedule set 1 to remote node 1, we could set:

Menu 11.1 - Remote Node Profile

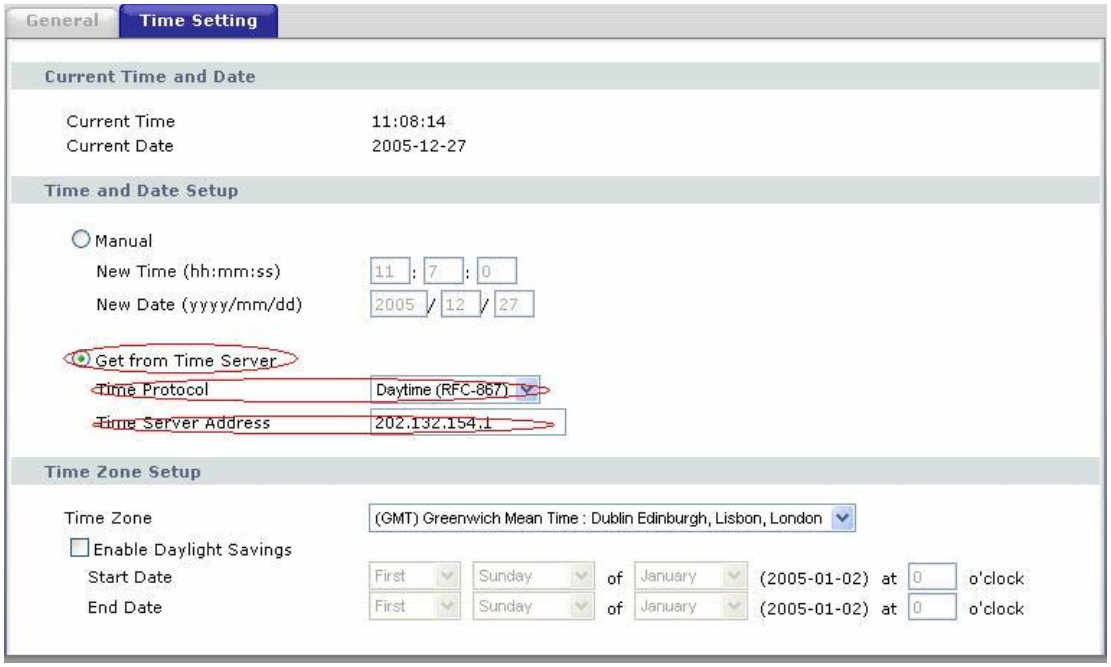
```
Rem Node Name= MyISP                Route= IP
Active= Yes                          Bridge= No

Encapsulation= PPPoE               Edit IP/Bridge= No
Multiplexing= LLC-based            Edit ATM Options= No
Service Name=                      Edit Advance Options= No
Incoming:                          Telco Option:
   Rem Login=                        Allocated Budget(min)= 0
   Rem Password= ********            Period(hr)= 0
Outgoing:                            Schedule Sets= 1
   My Login= user                    Nailed-Up Connection= No
   My Password= ********           Session Options:
   Authen= CHAP/PAP                  Edit Filter Sets= No
                                     Idle Timeout(sec)= 0
```

- Time Service in P-793H v2

There is no RTC (Real-Time Clock) chip so the P-793H v2 should launch a mechanism to get current time and date from external server in boot time. Time service is implemented by the **Daytime protocol (RFC-867)**, **Time**

All contents copyright © 2010 ZyXEL Communications Corporation.

Protocol (RFC-868), and **NTP protocol (RFC-1305)**. You have to assign an IP address of a time server and then, the P-793H v2will get the date, time, and time-zone information from this server. You can configure it in Web Configurator, Advanced Setup, **Maintenance -> System -> Time Setting.**



16. Using IP Multicast

What is IP Multicast ?

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. Host groups are identified by class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the P-793H v2 queries all directly connected networks to gather group membership.

After that, the P-793H v2 updates the information by periodic queries. The P-793H v2 implementation of IGMP is also compatible with version 1.
The multicast setting can be turned on or off on Ethernet and remote nodes.

All contents copyright © 2010 ZyXEL Communications Corporation.

- **IP Multicast Setup**

(1) Enable IGMP in P-793H v2's LAN in Web Configurator, Advanced Setup, **Network -> LAN -> IP -> Advanced Setup.**

(2) Enable IGMP in P-793H v2's remote node in Web Configurator, Advanced Setup, **Network -> Remote Node -> Edit -> Multicast.**

Key Settings:

Multicast	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2.

17. Using Bandwidth Management

- **Why Bandwidth Management (BWM)?**

Nowadays, we have many different traffic types for Internet applications. Some traffic may consume high bandwidth, such as FTP (File Transfer Protocol). Some other traffic may not require high bandwidth, but they require stable supply of bandwidth, such as VoIP traffic. The VoIP quality would not be good, if all of the outgoing bandwidth is occupied via FTP. Additionally, chances are that you would like to grant higher bandwidth for some body special who is using specific IP address in your network. All of these are reasons why we need bandwidth management.

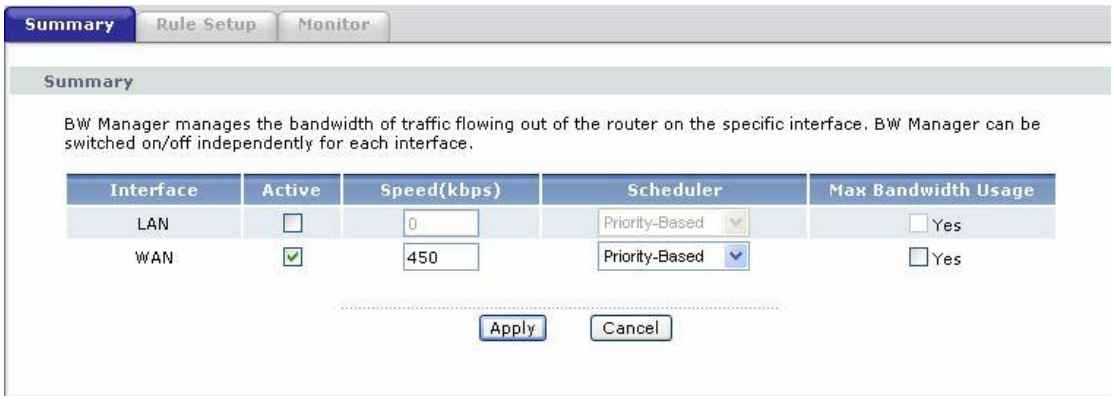
- **Using BWM**

Setp 1: Go to Web Configurator, Advanced Setup, **Advanced -> Bandwidth MGMT->Summary**, activate bandwidth management on the interface you would like to manage. We enable the BWM function on WAN interface in this example.

Enter the total speed for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class.

Select how you want the bandwidth to be allocated. **Priority-Based** means bandwidth is allocated via priority, so the traffic with highest priority would be served first, then the second priority is served secondly and so on. If **Faimess-Based** is chosen, then the bandwidth is allocated by ratio. Which means if A class needs 300 kbps, B class needs 600 kbps, then the ratio of A and B's actual bandwidth is 1:2. So if we get 450 kbps in total, then A would get 150 kbps, B would get 300 kbps. We select **Priority-Based** in this example.

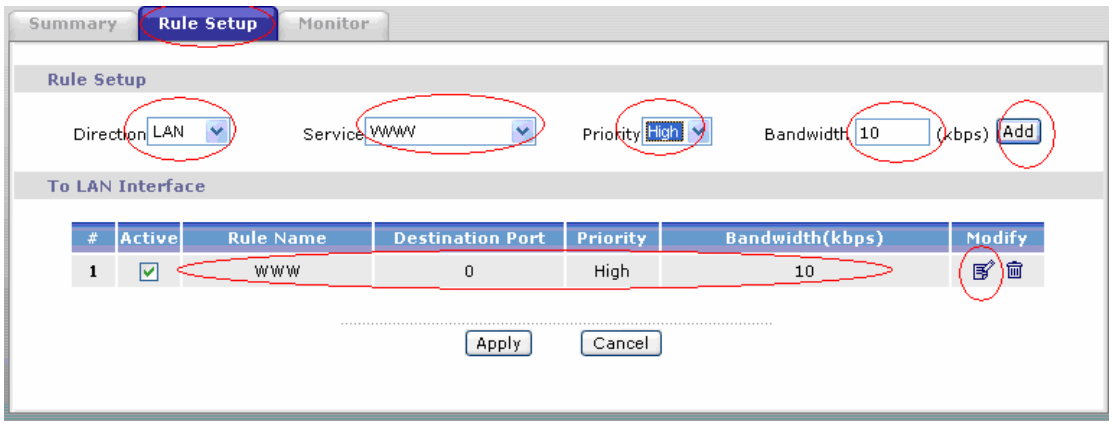
All contents copyright © 2010 ZyXEL Communications Corporation.



Key Settings:

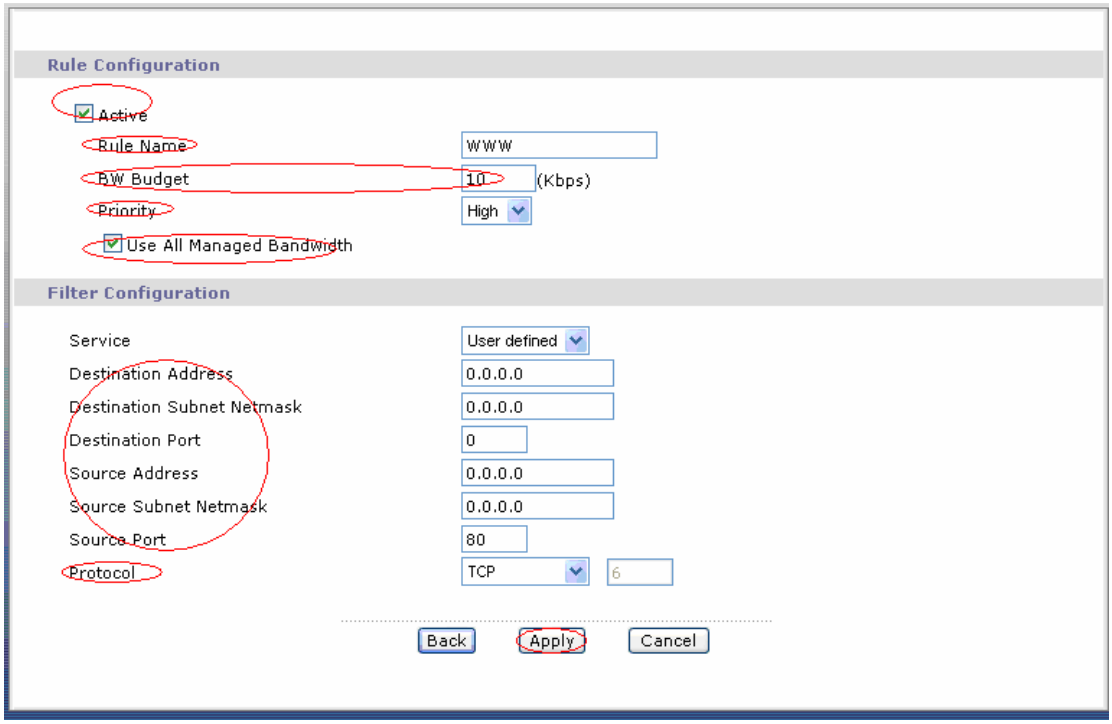
Active	Check the box to enable BWM on the interface. Note that if you would like to manage traffic from **WAN to LAN**, you should apply BWM on **LAN** interface.
Speed	Enter the total speed to manage on this interface. This value is the budget of the class tree's root.
Scheduler	Choose the principle to allocate bandwidth on this interface. **Priority-Based** allocates bandwidth via priority. **Fairness-Based** allocates bandwidth by ratio.
Maximize Bandwidth Usage	Check this box if you would like to give residuary bandwidth from Interface to the classes who need more bandwidth than configured amount. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the bandwidth of each class at the configured value. (Please note that to meat the second condition, you should also disable **Use All Managed Bandwidth** in the BWM rule.)

Step 2: Go to Web Configurator, Advanced Setup, **Advanced -> Bandwidth MGMT-> Rule Setup**, select the **interface, Service, Priority,** and Allocated **Bandwidth** for this rule, then click button '**Add**' to apply this rule.



Step 3: You can modify the rule by clicking the button **'Edit'** on the rule:

All contents copyright © 2010 ZyXEL Communications Corporation.



Key Settings:

RuleName	Give this rule a name, for example, **'WWW'**
BW Budget	Configure the bandwidth you would like to allocate to this rule
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Use All Managed Bandwidth	Check this box if you would like to let this class to borrow bandwidth from it's parents when the required bandwidth is higher than the configured amount. Do not check this if you want to limit the bandwidth of this class at the configured value.(Please note that you should also disable **Maximize Bandwidth Usage** on the interface to meet the condition.)
Service	Select **User-defined, SIP, FTP, or H.323** to specify the traffic types
Destination IP Address	Enter the IP address of destination that meets this class.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the destination port number of the traffic.
Source IP Address	Enter the IP address of source that meats this class. Note that for traffic from **'LAN to WAN'**, since BWM is before NAT, you should use the IP address before NAT processing.
Source Subnet Mask	Enter the destination subnet mask.

All contents copyright © 2010 ZyXEL Communications Corporation.

Source Port	Enter the source port number of the traffic.
Protocol ID	Enter the protocol number for the traffic. 1 for ICMP, 6 for TCP or 17 for UDP

After configuration BWM, you can check current bandwidth of the configured traffic in Web Configurator, Advanced Setup, **Advanced -> Bandwidth MGMT-> Monitor.**

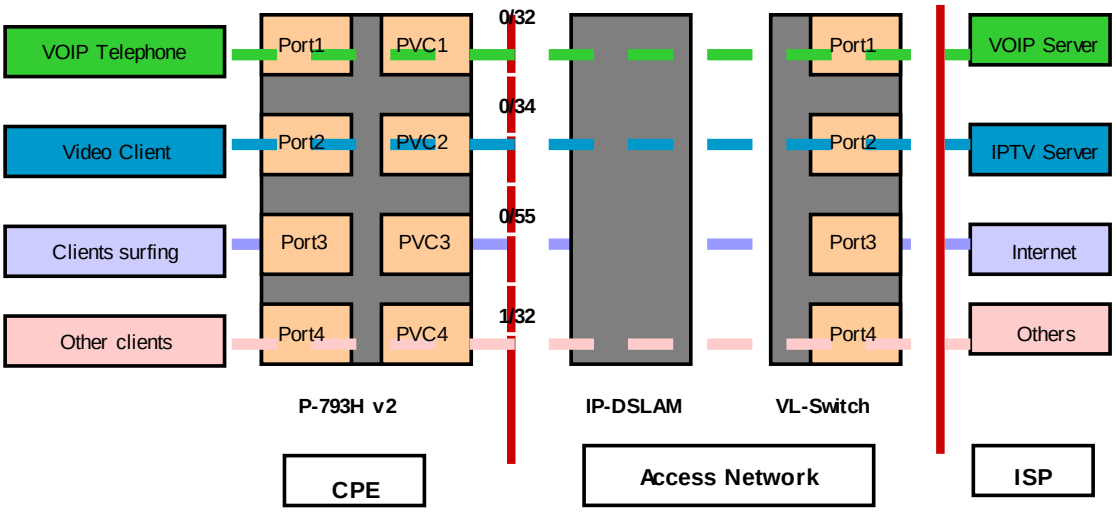
18. How to configure packet filter on P-793H v2?

The P-793H v2 allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

The packet filter on P-793H v2 is configured in SMT menu 21.1.

19. How could I configure triple play on P-793H v2?

The common triple play scenario is as follows:



Triple Play is a port-based policy to forward packets from different LAN port to different PVCs, thus we could assign different parameters to the PVC (**CBR, UBR, VBR-RT, VBR-nRT**) to guarantee different applications.

We could configure triple play on P-793H v2 in **SMT menu 24.8** as below**:**

8021Q groupset [groupid] [vid] [LAN] [index]|[PVC|WLAN|PWR|USB] [tagged/untagged]

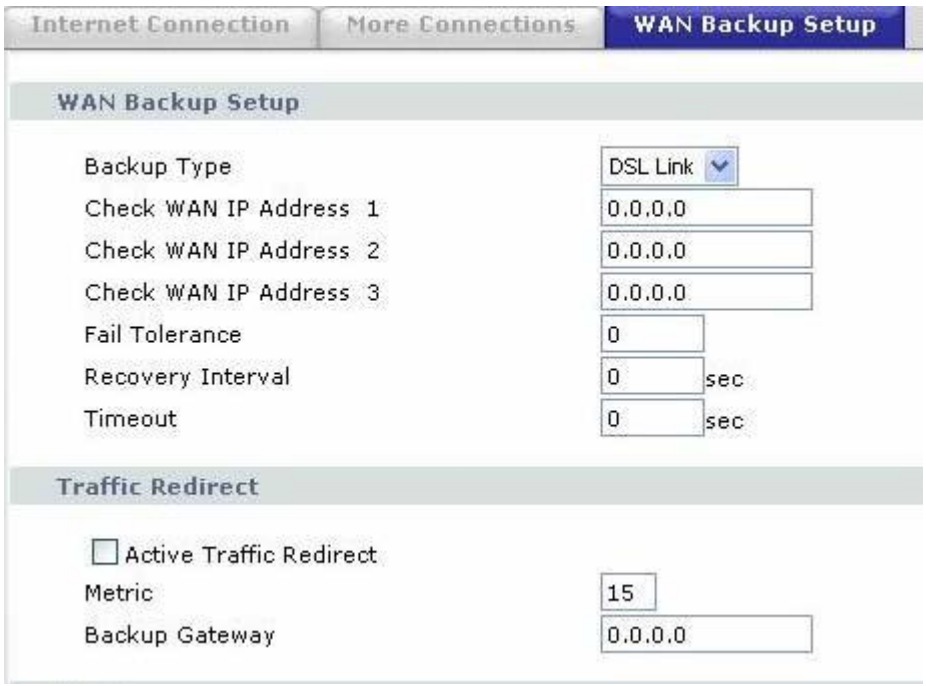
All contents copyright © 2010 ZyXEL Communications Corporation.

For example: **802 groupset 1 1 LAN 1 PVC 1 untagged**
802 groupset 2 2 LAN 2 PVC 2 untagged
802 groupset 3 3 LAN 3 PVC 3 untagged
The traffic from Ethernet port 1 must be forwarded to PVC1, vice versa.
The traffic from Ethernet port 2 must be forwarded to PVC2, vice versa.
The traffic from Ethernet Port 3 must be forwarded to PVC3, vice versa.

Note: Only the group vid matches management vid, PC in this group could manage the device.

20. How to setup traffic redirect in P-793H v2?

Configure parameters in WEB Configuration "**Network→ WAN→ Wan Backup"** as below**:**



WAN Backup Setup settings**:**

Backup Type: Select the method that the P-793H v2 uses to check the DSL connection. Select **DSL Link** to have the P-793H v2 check if the connection to the DSLAM is up. Select **ICMP** to have the P-793H v2 periodically ping the IP address configured in the **Check WAN IP Address** fields.

Check WAN IP Address 1-3: Configure the field to test your P-793H v2's WAN accessibility. When using a WAN backup connection, the P-793H v2 periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.

All contents copyright © 2010 ZyXEL Communications Corporation.

Fail Tolerance: Type the number of times (2 recommended) that your P-793H v2 may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection.

Recovery Interval: When the P-793H v2 is using a lower priority connection (usually a WAN Backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the P-793H v2 to wait between checks. Allow more time if your destination IP address handles lots of traffic.

Timeout: Type the number of seconds (3 recommended) for your P-793H v2 to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the P-793H v2 times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.

Traffic Redirect Settings:

Active: Enable or disable traffic redirect setup.

Backup Gateway: The IP address of your backup gateway. P-793H v2 automatically forwards outgoing traffic to this IP address if Prestige's Internet connection terminates.

Metric: Enter a number from 1 to 15 to give your traffic redirect route a priority number. The smaller the number, the higher priority the route has.

You can also configure WAN backup via **SMT Menu 2- WAN Setup** and traffic redirect via **SMT Menu 2.1- Traffic Redirect Setup.**

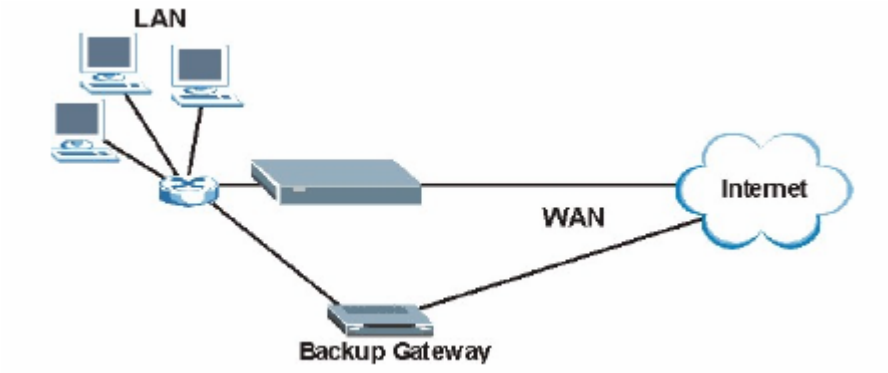
All contents copyright © 2010 ZyXEL Communications Corporation.

```
            Menu 2 - WAN Setup

        Service Mode= 2wire
        Service Type= Client
        Rate Adaption= N/A
        Transfer Max Rate(Kbps)= N/A
        Transfer Min Rate(Kbps)= N/A
        Standard Mode= N/A
        Wan Backup Setup:
          Check Mechanism = DSL Link
          Check WAN IP Address1 = 0.0.0.0
          Check WAN IP Address2 = 0.0.0.0
          Check WAN IP Address3 = 0.0.0.0
            KeepAlive Fail Tolerance = 0
            Recovery Interval(sec) = 0
            ICMP Timeout(sec) = 0
          Traffic Redirect = No
          Dial Backup = No
 Press ENTER to Confirm or ESC to Cancel:
```

```
     Menu 2.1 - Traffic Redirect Setup

Active= No
Configuration:
  Backup Gateway IP Address= 0.0.0.0
  Metric= 15
```

21. How to deal with Triangle Route and Traffic redirect?

Traffic redirect scenario:



(1). Triangle route introduction

All contents copyright © 2010 ZyXEL Communications Corporation.

A traffic route is a path for sending or receiving date packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

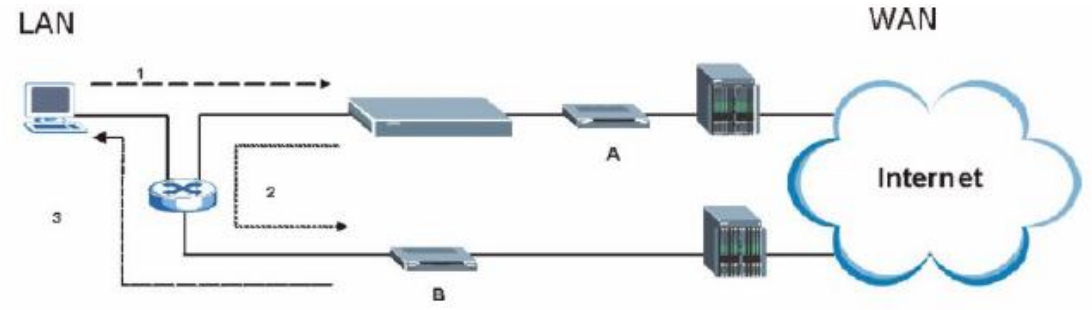
1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

2. The P-793H v2 reroutes the SYN packet through Gateway B on the LAN to the WAN.

3. The reply from WAN goes directly to the computer on the LAN without going through the P-793H v2.

As a result, the P-793H v2 resets the connection, as the connection has not been acknowledged.

“Triangle Route” Problem:



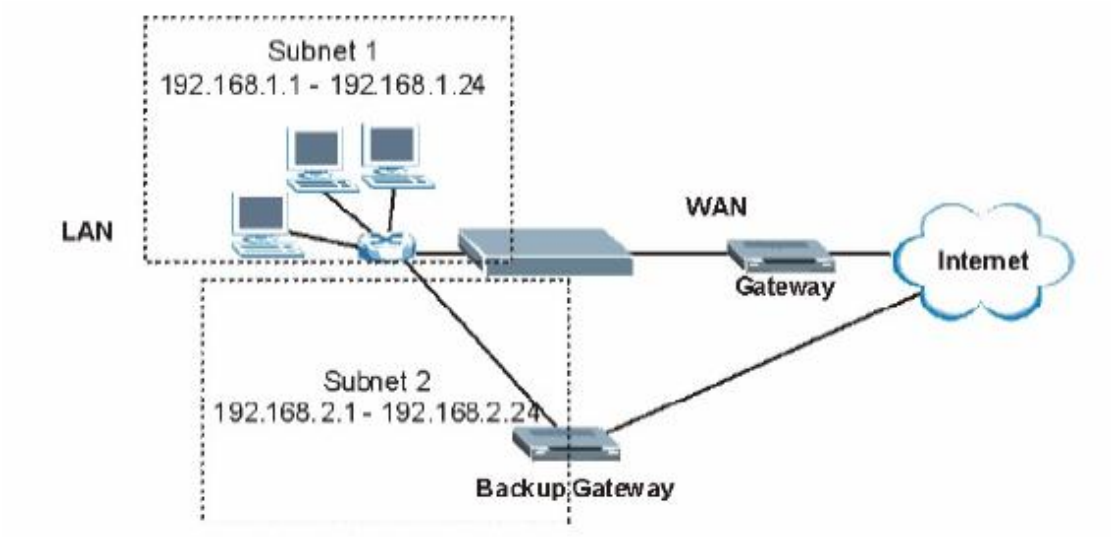
(2). How to avoid triangle route

1) IP Aliasing

The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the P-793H v2 itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

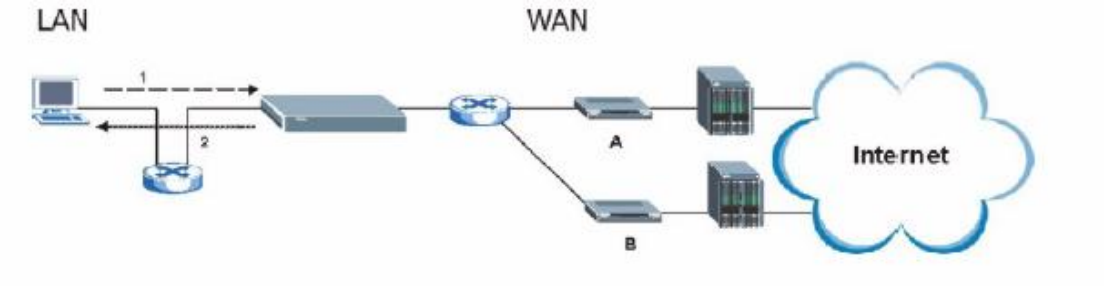
Traffic redirect LAN setup example 1:

All contents copyright © 2010 ZyXEL Communications Corporation.



2) Deploy your second gateway on WAN side

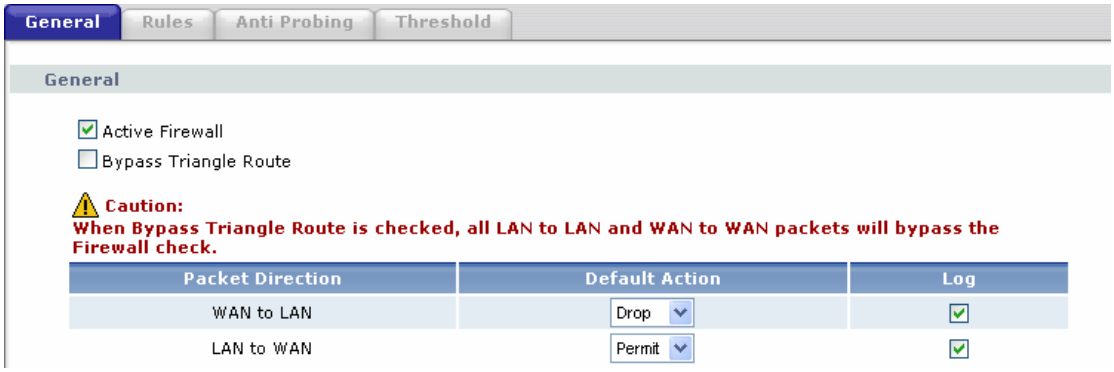
Put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your P-793H v2 to your LAN. Therefore your LAN is protected. Traffic redirect LAN setup example 2:



3) Allow firewall bypass triangle route checking

To resolve this conflict, we add an option for users to allow/disallow such Triangle Route topology in both CI command and Web configurator . You can issue command, "sys firewall ignore triangle all on" to allow firewall bypass triangle route checking. In Web GUI, you can find this option via "**Security**⇨ **Firewall**⇨ **General**".

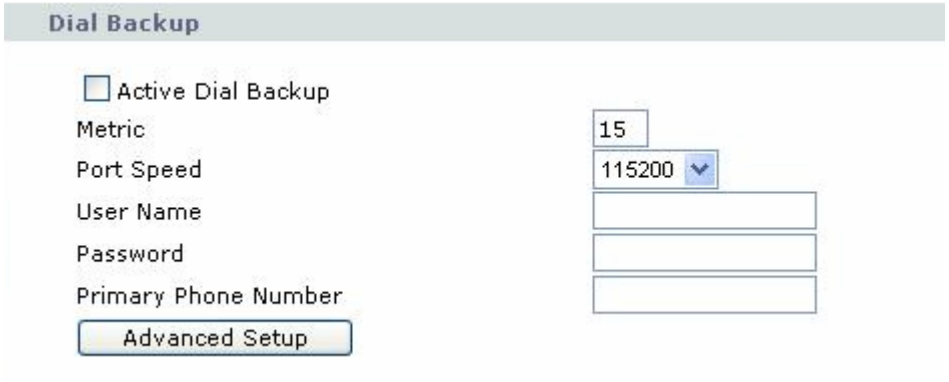
All contents copyright © 2010 ZyXEL Communications Corporation.



22. How to setup Dial Backup?

Please refer to **"20.How to setup traffic redirect in P-793H v2?" to** Configure parameters in WEB Configuration "**Network WAN Wan Backup".**

After finishing **WAN Backup Setup** settings, please do below configurations for dial backup:



Active: Turn on or off dial backup.

Metric: Enter a number from 1 to 15 to give your dial backup route a priority number. The smaller the number, the higher priority the route has.
Note: This field sets this router's priority among the three routes the P-793H v2 uses (normal, traffic redirect and dial backup). If the three routes have the same metrics, the priority of the routes is as follows:
WAN, Traffic Redirect, Dial Backup.
Port Speed: Use the drop-down list box to select the speed of the connection between the dial backup port and the external device.
User Name: Type the login name assigned by your ISP.
Password: Type the password assigned by your ISP.
Primary Phone Number: Type the first phone number from the ISP for this

All contents copyright © 2010 ZyXEL Communications Corporation.

remote node.
Advanced Setup: Click this button to display the **Advanced Setup** screen and edit more details of your WAN backup setup.(For more descriptions, please refer to User's Guide).

IPSEC VPN Application Notes

1. How to use P-793H v2 to build VPN Tunnel with another VPN Gateway/ Software?

This page will guide you to setup a VPN connection between two Prestige routers. In addition to Prestige to Prestige, Prestige can also talk to other VPN hardwards/softwares. The tested VPN hardwares are shown below:

- Cisco 1720 Router, IOS 12.2(2)XH, IP/ADSL/FW/IDS PLUS IPSEC 3DES
- NetScreen 5, ScreenOS 2.6.0r6
- SonicWALL SOHO 2
- WatchGuard Firebox II
- ZyXEL VPN solution
- Avaya VPN
- Netopia VPN
- III VPN

The tested VPN softwares are shown below:

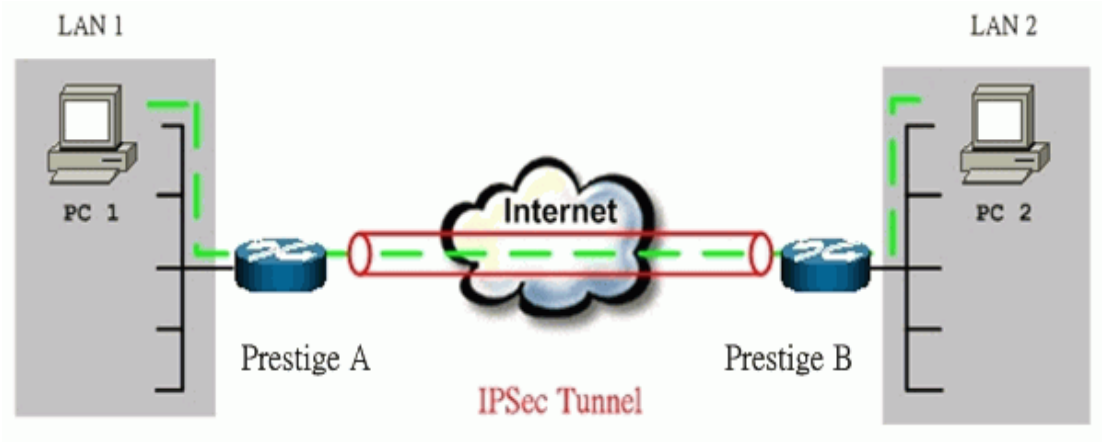
- Checkpoint VPN software
- WIN2K VPN software
- Soft-PK VPN software
- Linux FreeS/WAN VPN
- SSH Sentinel
- Intel VPN client software

Let's focus on the how to configure VPN tunnel on Prestige now:

- **Prestige to Prestige Tunnel**

All contents copyright © 2010 ZyXEL Communications Corporation.

As the figure shown below, the tunnel between Prestige 1 and Prestige 2 ensures the packets flow between PC 1 and PC 2 are secure. Because the packets go through the IPSec tunnel are encrypted. To achieve this VPN tunnel, the settings required for each Prestige are explained in the following sections.



The IP addresses we use in this example are as below.

PC 1	Prestige A	Prestige B	PC 2
192.168.1.33	LAN: 192.168.1.1 WAN:	LAN: 192.168.2.1 WAN:	192.168.2.33

Note: The following configurations are supposed both two VPN gateways have fixed IP addresses. If one of VPN gateways uses dynamic IP, we enter **0.0.0.0** as the secure gateway IP address. In this case, the VPN connection can only be initiated from dynamic side to fixed side to update its dynamic IP to the fixed side. If both of VPN gateways use dynamic IP, we need DDNS service to implement it.

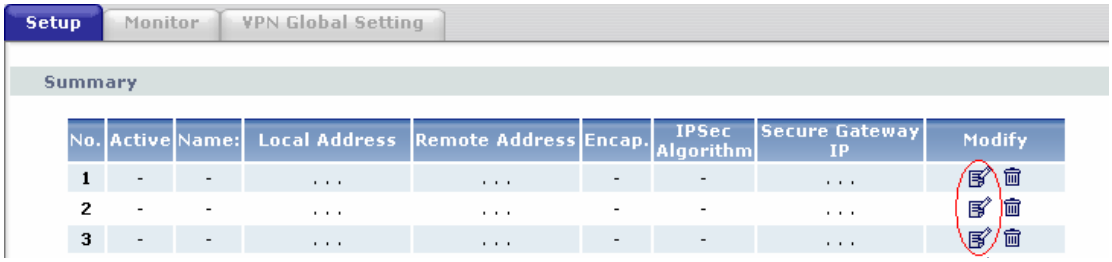
You can finish the configuration via Web Configurator on Prestige:

Step 1: Set up Prestige A

(1) Using a web browser, login Prestige Web Configurator by giving the LAN IP address of Prestige in URL field. Default LAN IP is **192.168.1.1**, default password to login advanced web configurator is **1234**.

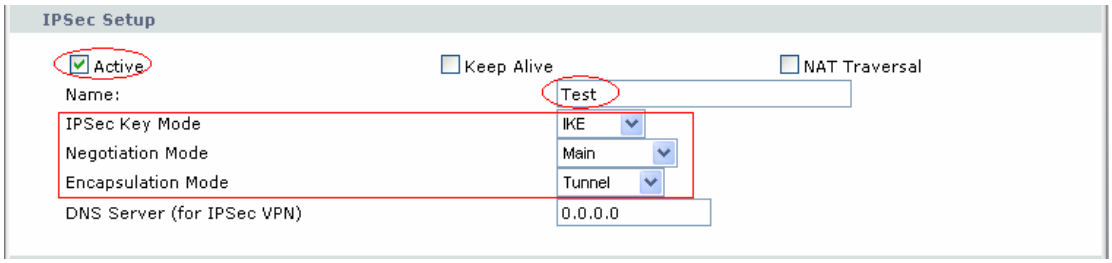
(2) Go to VPN Setup page to edit a VPN Rule. On P-793H v2, you could begin with **Security -> VPN -> Summery:**

All contents copyright © 2010 ZyXEL Communications Corporation.



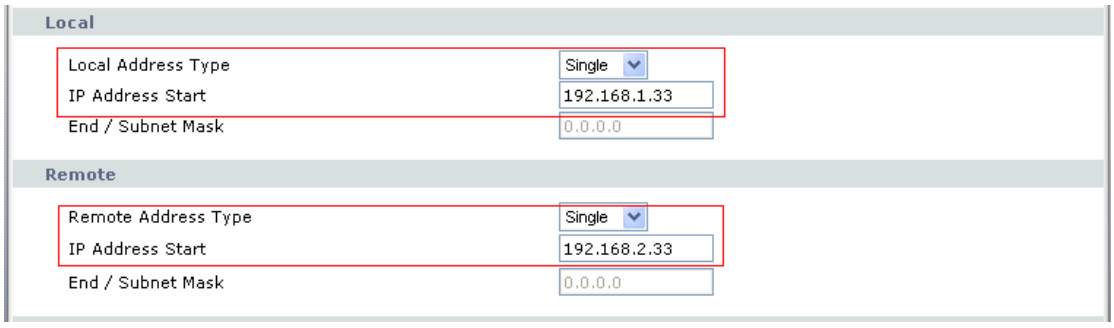
(3) On the **SUMMARY** menu, select a policy to edit by clicking **Edit**. On P-793H v2, we can build at most 2 VPN Tunnels. Just make a click on the '**Edit**' button in the table, we can begin to configure the VPN rule.

(4) In the **IPSEC Setup** field, toggle **Active** check box and give a name, **Test** in the example to this policy.
Select **IPSec Key Mode** to **IKE, Negotiation Mode** to **Main**, and **Encapsulation Mode** to **Tunnel**, just the same as we will configure in Prestige B.



(5) Fill in the Local and Remote secure hosts information in the **Local** and **Remote** field.

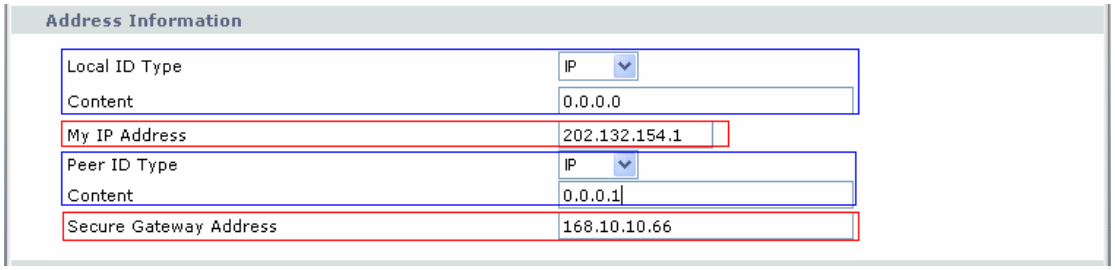
Local Address Type is **Single** and **IP Address Start** is **PC 1's IP**, **192.168.1.33** in the example.
Remote Address Type is **Single** and **IP Address Start** is **PC 2's IP**, **192.168.2.33** in the example.



(6) Fill in the VPN Gateway information in the **Address Information** field.

All contents copyright © 2010 ZyXEL Communications Corporation.

My IP Address is the **WAN IP of Prestige A**, **202.132.154.1** in the example.
Secure Gateway Address is the remote secure gateway, **Prestige B's WAN IP**, **168.10.10.66** in the example.
Local ID Type as **IP**, and **Content** as **0.0.0.0** in the example.
Peer ID Type as **IP**, and **Content** as **0.0.0.1** in the example.

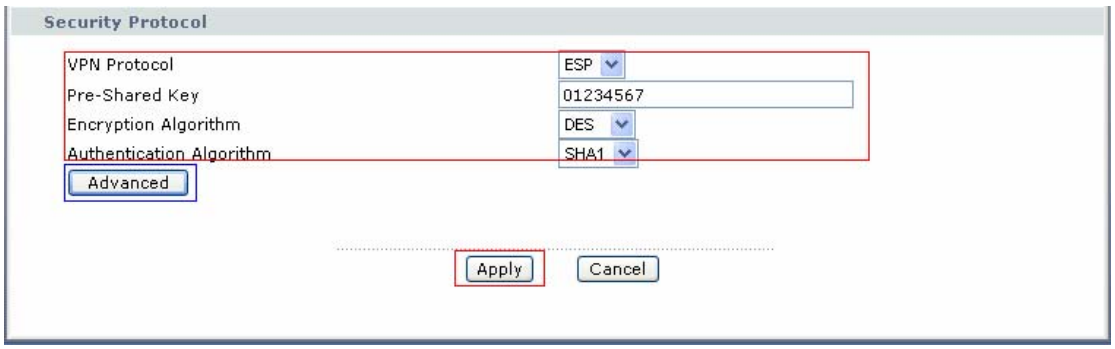


Note: Make sure the ID Type and content consistent between the two VPN secure gateways. As in the example, we've finished this field on Prestige A, then when we configure Prestige B, we should make it fit the following table:

	Prestgie A	Prestige B
Local ID Type	IP	IP
Content	0.0.0.0	0.0.0.1
Peer ID Type	IP	IP
Content	0.0.0.1	0.0.0.0

(7) Fill in VPN Protocol, Pre-Shared Key, Encryption Algorithm, Authentication Algorithm in the **Security Protocol** field

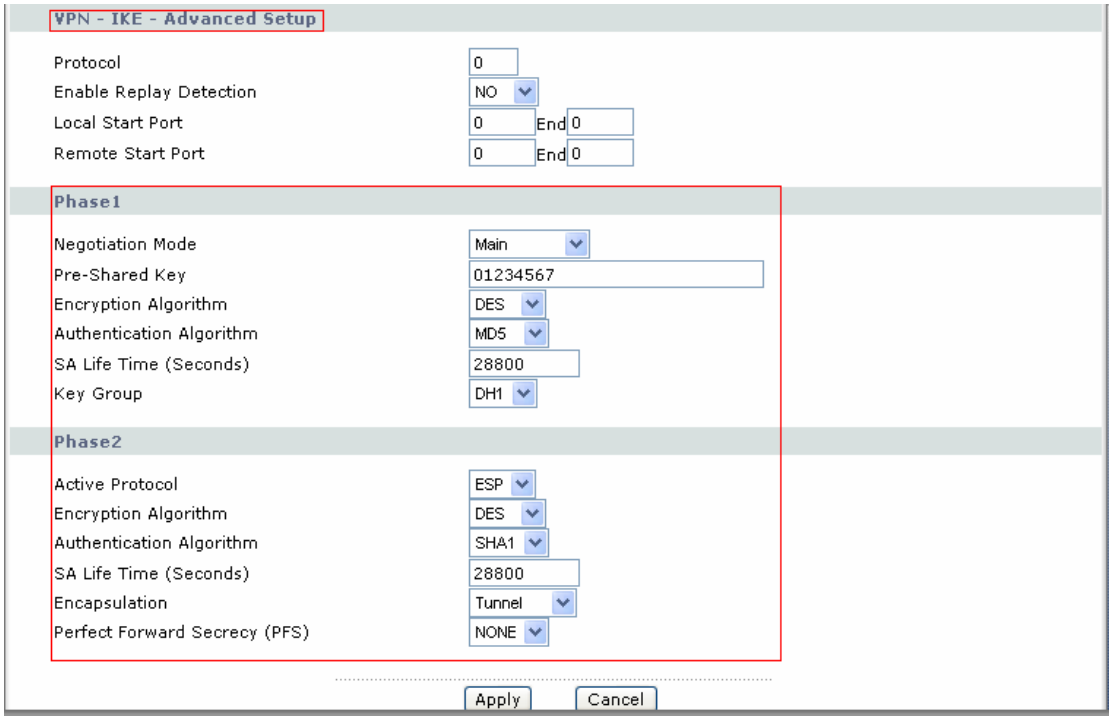
Select one **VPN Protocol** from the pull-down menu, **ESP** in the example.
Input a proper **Pre-Shared Key** in the right table, 01234567 in the example.
Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**.



All contents copyright © 2010 ZyXEL Communications Corporation.

Note: If there's a NAT router between the two VPN Secure Gateways, we should only choose '**ESP**' VPN Protocol. The minimum length of **Pre-Shared Key** is **8**.

(8) A common VPN Rule has been completed, you can click 'Apply' to save it. But if you want to make more special configuration, you could click 'Advanced' to continue:



Note: If you make any change in advanced setup, you need to configure the same on Prestige B.

We don't do any advanced setup in the example. Then we have finished the configuration on Prestige A.

Step 2: Setup Prestige B

Similar to the settings for Prestige A, Prestige B is configured in the same way except that:
(1) **Local Address Type** is **Single** and **IP Address Start** is **PC 2's IP**, **192.168.2.33** in the example.
Remote Address Type is **Single** and **IP Address Start** is **PC 1's IP**, **192.168.1.33** in the example.

(2) **My IP Address** is the **WAN IP of Prestige B**, **168.10.10.66** in the example.

All contents copyright © 2010 ZyXEL Communications Corporation.

Secure Gateway Address is the remote secure gateway, **Prestige A's WAN IP**, **202.132.154.1** in the example.

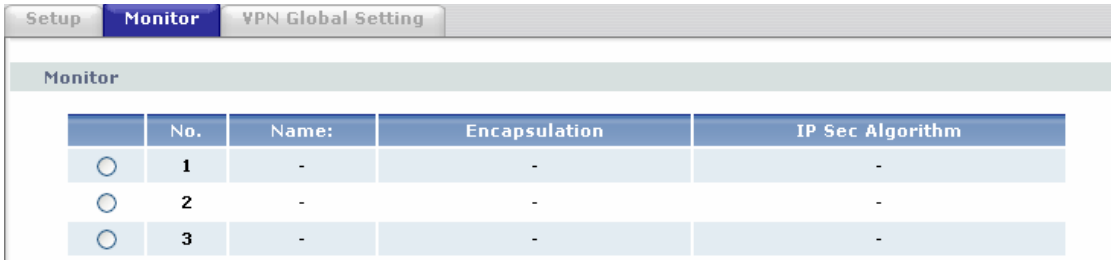
(3) **Local ID Type /Content** should be the same as **Prestige A's Peer ID Type/Content**, **IP/0.0.0.1** in the example.
Peer ID Type /Content should be the same as **Prestige A's Local ID Type/ Content**, **IP/0.0.0.0** in the example.

Step 3: Verify if the VPN Tunnel has been established successfully

If the connection between PC 1 and PC 2 is ok, we know the tunnel works. Please try to ping from PC 1 to PC 2 (or PC 2 to PC 1). If PC 1 and PC 2 can ping to each other (ping **192.168.2.33** or **192.168.1.33** in the example), it means that the IPSec tunnel has been established successfully. If the ping fails, there are two methods to troubleshoot IPSec in Prestige:

(1) Check the VPN Monitor

On P-793H v2 Web Configurator, **Security -> VPN -> Monitor,** you can check every active IPSec connections. The VPN Name, Encapsulation, and IPSec Algorithm will be shown in the Monitor Table. If you can't see the name of your IPSec rule, it means that the SA establishment fails. You need to go to the VPN Setup Page to check your settings.



- Use CI command **'ipsec debug on'**

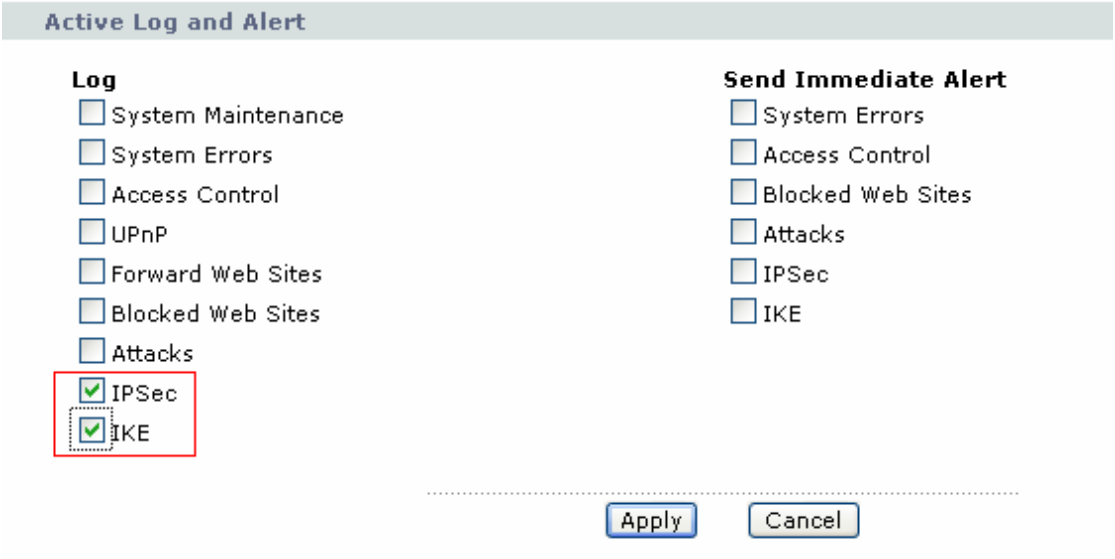
If the Monitor shows that the VPN tunnel has been established successfully, but the PC1 and PC 2 can't reach each other. We can invoke command '**ipsec debug 1**' in CLI for trouble shooting. There should be lots of detailed messages printed out to show how negotiations are taken place. If IPSec connection fails, please dump 'ipsec debug 1' and send the dump information to Support Engineer for a solution. The following shows an example of dumped messages. (You can refer to Support Tool -> 1 WAN/ LAN Packet Trace -> Capture the detailed logs by Hyper Terminal to do it).

All contents copyright © 2010 ZyXEL Communications Corporation.

```
Prestige> ipsec debug 1
IPSEC debug level 1
Prestige> catcher(): recv pkt numPkt<1>
get_hdr nxt_payload<1> exchMode<2> m_id<0> len<80>
f76af206 b187aae3 00000000 00000000 01100200 00000000 00000050 00000034
00000001 00000001 00000028 01010001 00000020 01010000 80010001 80020001
80040001 80030001 800b0001 800c0e10
In isadb_get_entry, nxt_pyld=1, exch=2
New SA
```

(2) View IPSec Log

We can also view the log for IPSec and IKE connections for trouble shooting. On P-793H v2, we can check the logs via **Web Configurator** or **CLI**. The log menu is also useful for troubleshooting please capture to us if necessary. For example: Select **IPSec** and **IKE** in Web Configurator, **Maintenance -> Logs -> Log Settings**



Then after a successful or failed VPN connection, we could view the relevant information from Web Configurator, **Maintenance -> Logs -> View Log:**

2. How to build a VPN between Secure Gateway with Dynamic WAN IP Address?

All contents copyright © 2010 ZyXEL Communications Corporation.

Most of the cases, static IP addresses are used for VPN tunneling endpoints. But for SOHO users, generally, it is a dynamic case. In this case, this IP will not be available to be predefined in the VPN box. There are some tips when configure Prestige in any dynamic case.

- **Prestige static WAN IP v.s. peer side dynamic IP**

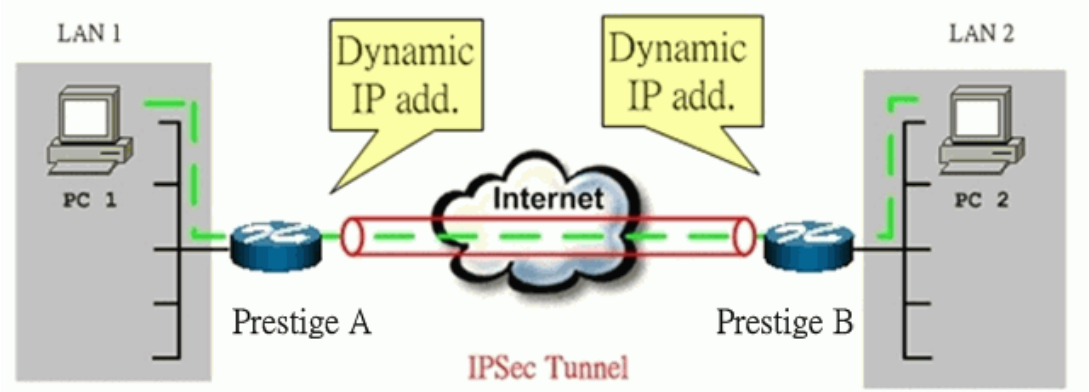
We need to note:
(1) In VPN settings of Prestige, please specify the IP address of **Secure Gateway** as **0.0.0.0**
(2) The VPN connection can **ONLY** be initiated from dynamic side to static side in order to update its dynamic IP to the static side.
(3) In peer side, are you using **Win2K built-in IPSec**? In this case, W2K won't capture the dynamic IP address automatically for you. You have to obtain your dynamic IP address and then go back to IPSec configuration to setup your current IP address.

- **Prestige dynamic WAN IP v.s. peer side static IP**

We need to note:
(1) In VPN settings of Prestige, please specify the IP address of **My IP** as **0.0.0.0**. Prestige will automatically bind it's current WAN IP address to IPSec.
(2) IPSec tunnel in this case, can **ONLY** be initiated from Prestige.
(3) In peer side, are you using **SonicWALL, NetScreen?** SonicWALL requires you to enter an ID (in FQDN format) to identify Prestige.

- **Prestige dynamic WAN IP v.s. peer side dynamic IP**

In this case, we need to use DDNS (Dynamic Domain Name Service). There are many different solutions for it:
(1) Prestige v.s. Prestige



All contents copyright © 2010 ZyXEL Communications Corporation.

Solution 1:

Step 1: In Prestige A, please register a DDNS account from http://www.dyndns.org or http://dynupdate.no-ip.com

Setp 2: Enable **DynDNS** function on Prestige A via Web configurator, **Advanced -> Dynamic DNS**. And in VPN settings on Prestige A, please specify the IP address of **My IP** as **0.0.0.0** and **Secure Gateway** as **0.0.0.0** (Here we take P-793H v2 Web Configurator as the example).

Step 3: In Prestige B, please specify the IP address of **My IP** as **0.0.0.0** and **Secure Gateway** as the domain name you registered for Prestige A.

Step 4: Please always initiate VPN tunnel from Prestige B on which Secure Gateway is configured as dynamic domain name.

Solution 2:

Step 1: Register DynDNS account from http://www.dyndns.org or http://dynupdate.no-ip.com for both PrestigeA & PrestigeB.

Step 2: In PrestigeA, configure **My IP** as **0.0.0.0** and **Secure Gateway** as the dynamic domain name of PrestigeB.

Step 3: In PrestigeB, configure **My IP** as **0.0.0.0** and **Secure Gateway** as the dynamic domain name of PrestigeA.

Step 4: You can initiate VPN tunnel from PrestigeA or PrestigeB by this solution.

(2) Prestige v.s. 3rd Party

This is highly dependent on which kind of 3rd party you use. Generally speaking, this 3rd party VPN solution must support either of the two items:

- Support DDNS for update of its dynamic WAN IP. (If Prestige is to be the VPN initiator)
- Support Secure Gateway can be configured by Domain Name. (If Prestige is to be the VPN responder)

3. Configure NAT for internal servers

Some tips for this application:

All contents copyright © 2010 ZyXEL Communications Corporation.

Generally, without IPSec, to configure an internal server for outside access, we need to configure the server private IP and its service port in SUA/NAT Server Table. The NAT router then will forward the incoming connections to the internal server according to the service port and private IP entered in SUA/NAT Server Table.

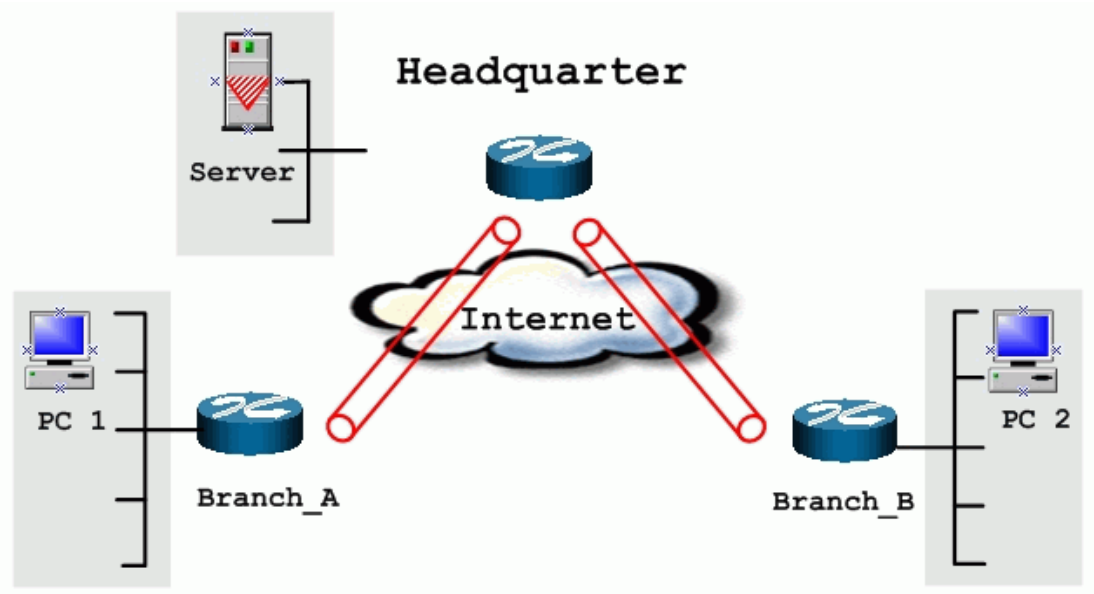
However, if both NAT and IPSec is enabled in Prestige, the edit of the table is necessary only if the connection is a non-secure connections. For secure connections, none SUA server settings are required since private IP is reachable in the VPN case. Remember, IPSec is an IP-in-IP encapsulation, the internal IP header is not translated by NAT. For example:
Internal Server----Prestige (NAT+IPSec)-----ADSL Modem----Internet----Remote Network

4. VPN Routing between Branch Office through Headquarter

This page guides us how to setup VPN routing between branch offices through headquarter. So that whenever branch office A wants to talk to branch office B, headquarter plays as a VPN relay. Users can gain benefit from such application when the scale of branch offices is very large, because no additional VPN tunnels between branch offices are needed. In this support note, we skip the detailed configuration steps for Internet access and presume that you are familiar with basic ZyNOS VPN configuration.

As the figure shown below, each branch office have a VPN tunnel to headquarter, thus PCs in branch offices can access systems in headquarter via the tunnel. Through VPN routing, Prestige series now provide you a solution to let PCs in branch offices talk to each other through the existing VPN tunnels concentrated on the headquarter.

All contents copyright © 2010 ZyXEL Communications Corporation.



The IP addresses we use in this example are as shown below.

Branch_A	Headquarter	Branch_B
WAN:202.3.1.1 LAN:192.168.3.1	WAN:202.1.1.1 LAN:192.168.1.1	WAN:202.2.1.1 LAN:192.168.2.1
LAN of Branch_A	**LAN of Headquarter**	**LAN of Branch_B**
192.168.3.0/24	192.168.1.0/24	192.168.2.0/24

Setp 1: Setup VPN in branch office A

Because VPN routing enables branch offices to talk to each other via tunnels concentrated on headquarter. In this step, we configure an IPSec rule in Prestige (Branch_A) for PCs behind branch office A to access both LAN segments of headquarter and branch office B. Because the LAN segments of headquarter and branch office B are continuous, we merge them into one single rule by including these two segments in **Remote** section. If by any chance, the two segments are not continuous, we strongly recommend you to setup different rules for these segments.

Create a VPN Rule with name **Branch_A**. The configuration is the same as Prestige to Prestige Tunnel, just the IP Address is a little different:

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.3.0, IP Address End** is **192.168.3.255.** This section covers the LAN segment of branch office A.

All contents copyright © 2010 ZyXEL Communications Corporation.

Remote Address Type is **Range Address** and **IP Address Start** is **192.168.1.0**, IP Address End is **192.168.2.255**. This section covers the LAN segment of both headquarter and branch office B.

(2) **My IP Address** is the WAN IP of Prestige in **Branch_A**, **202.3.1.1** in the example.
Secure Gateway Address is **IP address of Headquarter**, **202.1.1.1** in the example.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don't make any advanced setup in the example.

Step 2: Setup VPN in branch office B

Be very careful about the remote IP address in branch office B, because systems behind branch office B want to access systems behind branch office A and headquarter, we have to specify these two segments in **Remote** section. However if we include these two segments in one rule, the LAN segment of branch office B will be also included in this single rule, which means intercommunication inside branch office B will run into VPN tunnel. To avoid such situation, we need two separate rules to cover the LAN segment of branch office A and headquarter.

- **The first rule in Branch_ B, Branch_B_1.**

This rule is for branch office B to access headquarter.

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.2.0, IP Address End** is **192.168.2.255.** This section covers the LAN segment of branch office B.

Remote Address Type is **Range Address** and **IP Address Start** is **192.168.1.0**, IP Address End is **192.168.1.255**. This section covers the LAN segment of headquarter office.

(2) **My IP Address** is the WAN IP of Prestige in **Branch_B**, **202.2.1.1** in the example.
Secure Gateway Address is **IP address of Headquarter**, **202.1.1.1** in the example.

All contents copyright © 2010 ZyXEL Communications Corporation.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don't make any advanced setup in the example.

All contents copyright © 2010 ZyXEL Communications Corporation.

Support Tool

1. LAN/WAN Packet Trace

The P-793H v2 packet trace records and analyzes packets running on LAN and WAN interfaces. It is designed for users with technical backgrounds who are interested in the details of the packet flow on LAN or WAN end of P-793H v2. It is also very helpful for diagnostics if you have compatibility problems you're your ISP or if you want to know the details of a packet for configuring a filter rule. The format of the display is as following Packet:

[index] [timer/second][channel-receive/transmit][length] [protocol] [sourceIP/port] [destIP/port]

There are two ways to dump the trace:

Online Trace--display the trace real time on screen

Offline Trace--capture the trace first and display later

The details for capturing the trace in CLI as follows:

First of all, you need to telnet to the P-793H v2 firstly. The password is Administrator passwords, 'admin' by default.

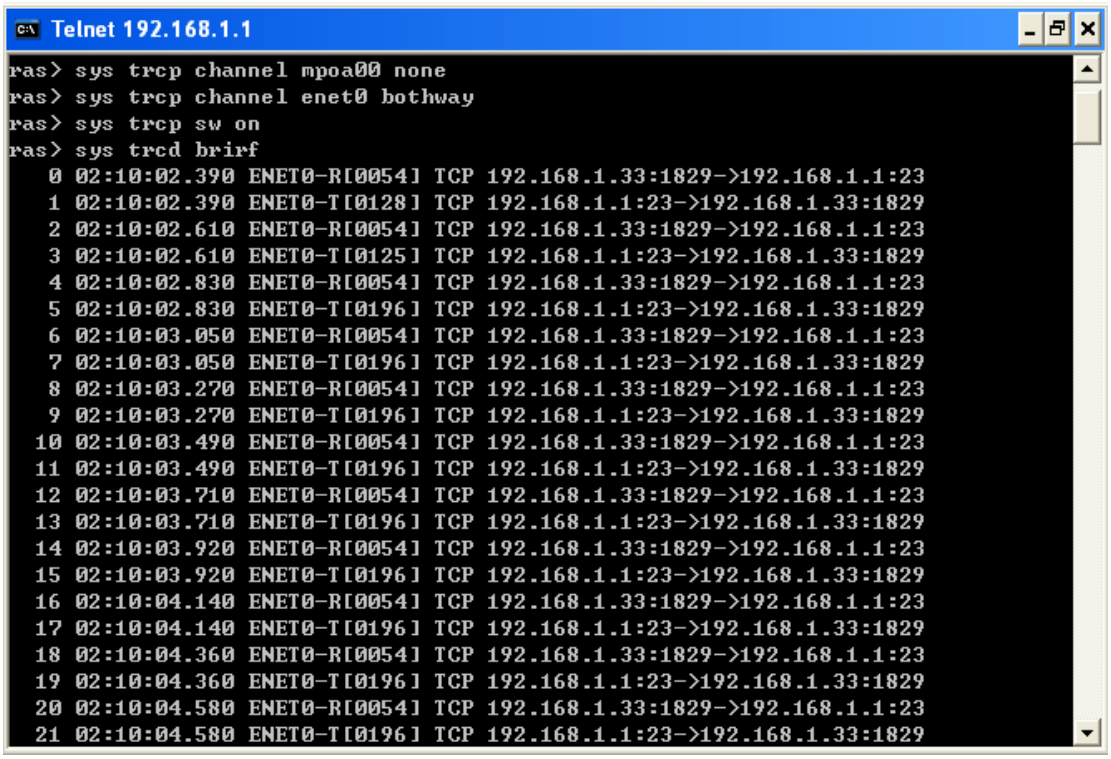
- **Online Trace**

(1) Trace LAN packet

- Disable to capture the WAN packet by entering: **sys trcp channel mpoa00 none**
- Enable to capture the LAN packet by entering: **sys trcp channel enet0 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Display the brief trace online by entering: **sys trcd brief**
- Display the detailed trace online by entering: **sys trcd parse**

Example:

All contents copyright © 2010 ZyXEL Communications Corporation.

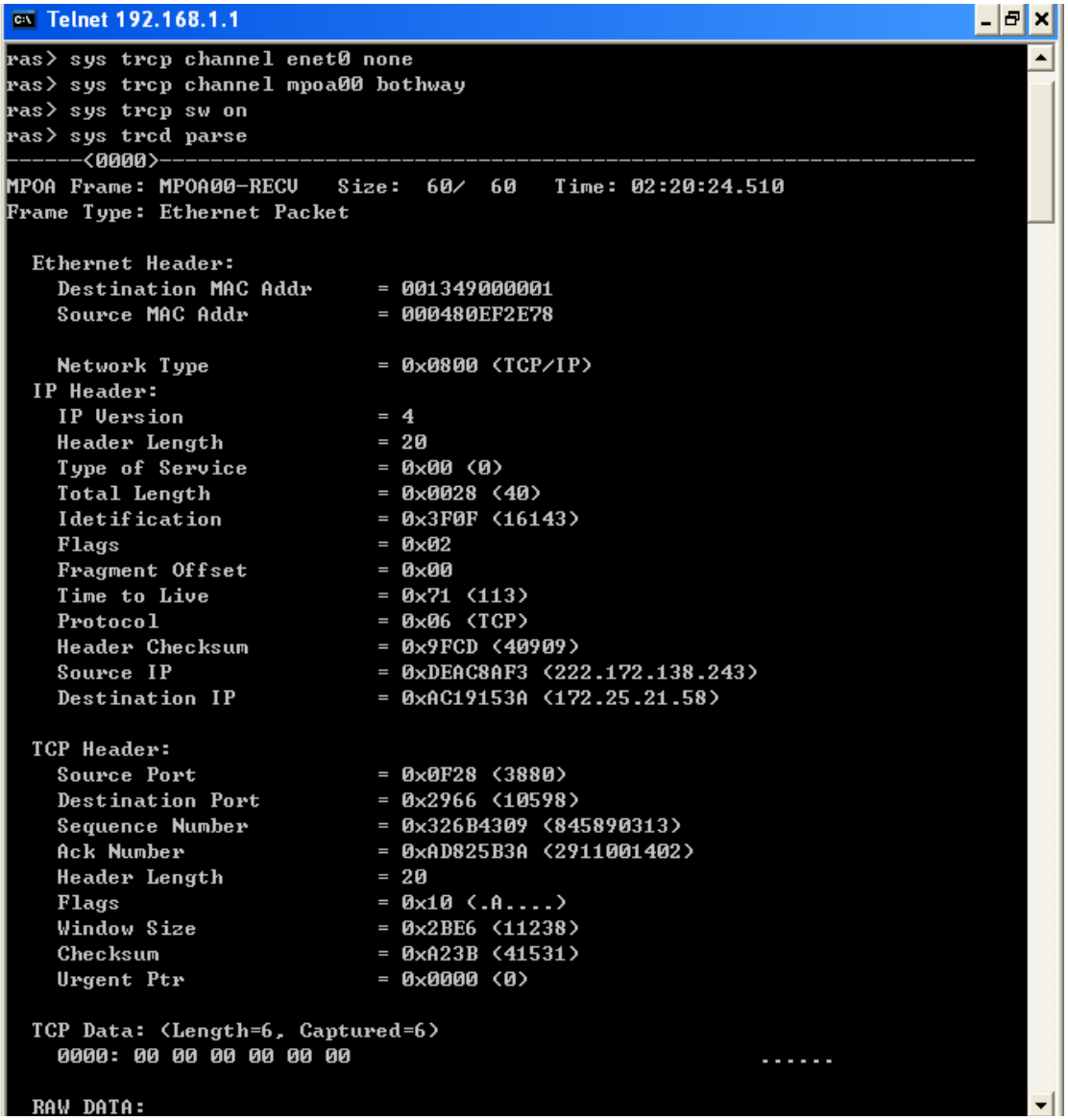


(2) Trace WAN packet

- Disable the capture of the LAN packet by entering: **sys trcp channel enet0 none**
- Enable to capture the WAN packet by entering: **sys trcp channel mpoa00 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Display the brief trace online by entering: **sys trcd brief**
- Display the detailed trace online by entering: **sys trcd parse**

Example:

All contents copyright © 2010 ZyXEL Communications Corporation.


Telnet 192.168.1.1
ras> sys trcp channel enet0 none
ras> sys trcp channel mpoa00 bothway
ras> sys trcp sw on
ras> sys trcd parse
------<0000>----------
MPOA Frame: MPOA00-RECV Size: 60/ 60 Time: 02:20:24.510
Frame Type: Ethernet Packet
Ethernet Header:
Destination MAC Addr = 001349000001
Source MAC Addr = 000480EF2E78
Network Type = 0x0800 (TCP/IP)
IP Header:
IP Version = 4
Header Length = 20
Type of Service = 0x00 (0)
Total Length = 0x0028 (40)
Idetification = 0x3F0F (16143)
Flags = 0x02
Fragment Offset = 0x00
Time to Live = 0x71 (113)
Protocol = 0x06 (TCP)
Header Checksum = 0x9FCD (40909)
Source IP = 0xDEAC8AF3 (222.172.138.243)
Destination IP = 0xAC19153A (172.25.21.58)
TCP Header:
Source Port = 0x0F28 (3880)
Destination Port = 0x2966 (10598)
Sequence Number = 0x326B4309 (845890313)
Ack Number = 0xAD825B3A (2911001402)
Header Length = 20
Flags = 0x10 (.A....)
Window Size = 0x2BE6 (11238)
Checksum = 0xA23B (41531)
Urgent Ptr = 0x0000 (0)
TCP Data: (Length=6, Captured=6)
0000: 00 00 00 00 00 00 ......
RAW DATA:

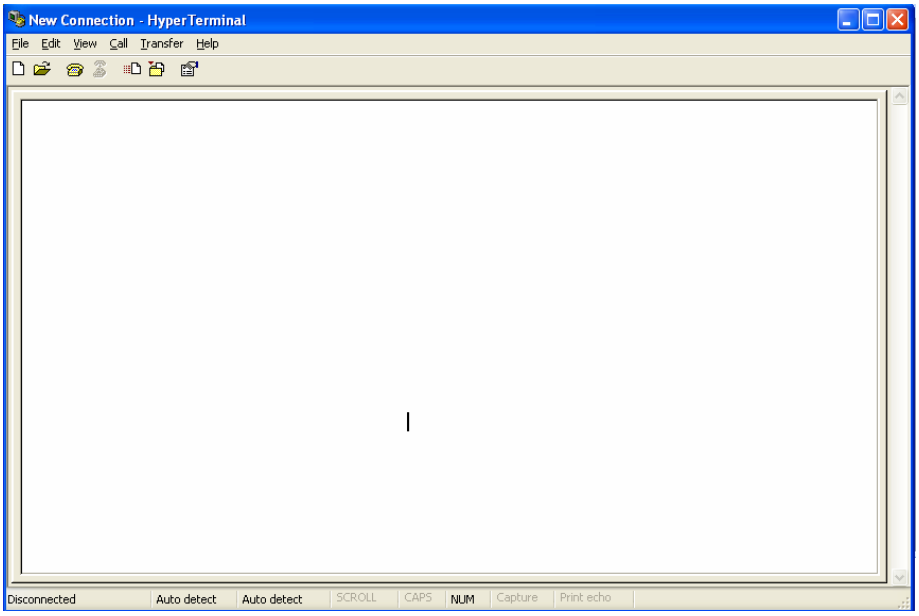
Offline Trace

- Disable the capture of the WAN packet by entering: **sys trcp channel mpoa00 none**
- Enable the capture of the LAN packet by entering: **sys trcp channel enet0 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Wait for packet passing through the P-793H v2 over LAN
- Disable the trace log by entering: **sys trcp sw off** & **sys trcl sw off**
- Display the trace briefly by entering: **sys trcp brief**
- Display specific packets by using: **sys trcp parse <from_index> <to_index>**

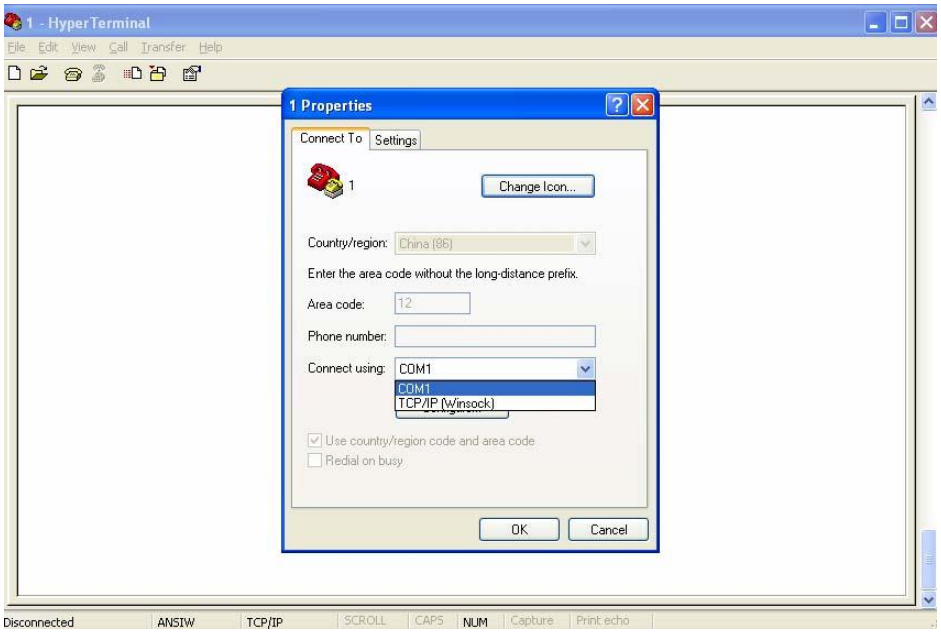
All contents copyright © 2010 ZyXEL Communications Corporation.

Capture the detailed logs by Hyper Terminal

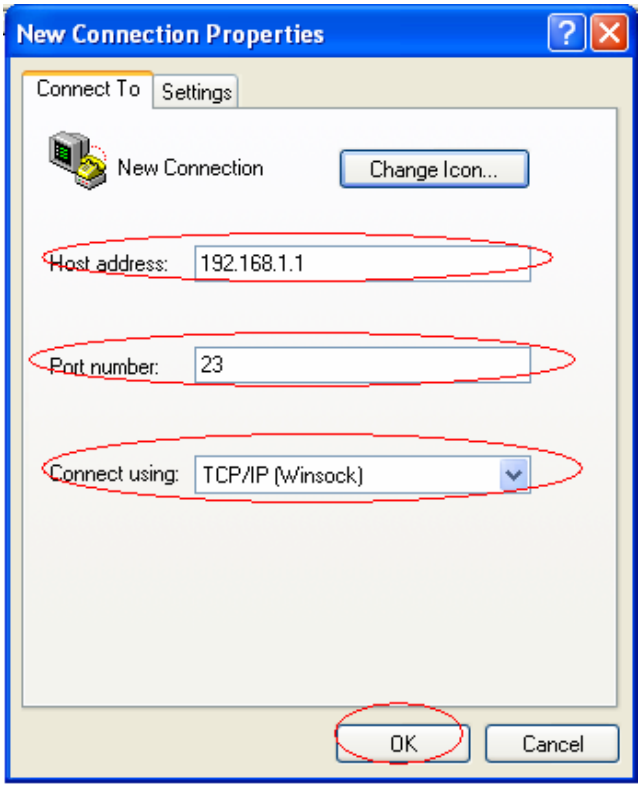
Step 1: Initiate a hyper terminal connection from your PC(suppose you connected to the LAN port of P-793H v2)



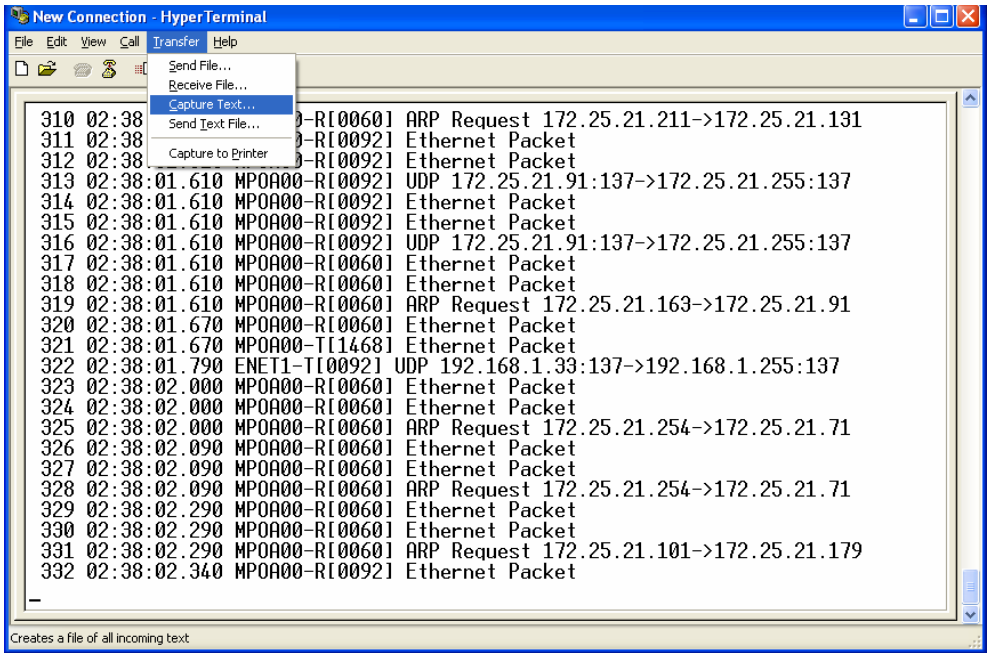
Step 2: Click the 'properties' to configure parameters to telnet to the P-793H v2.



All contents copyright © 2010 ZyXEL Communications Corporation.



Step 3: So that after you invoke the relevant commands, you could save the logs you've captured.



2. Firmware/Configurations Uploading and Downloading using TFTP

All contents copyright © 2010 ZyXEL Communications Corporation.

Using TFTP client software

- Upload/download ZyNOS via LAN
- Upload/download P-793H v2 configurations via LAN

(1) Using TFTP to upload/download ZyNOS via LAN

Step 1: TELNET to your P-793H v2 first before running the TFTP software

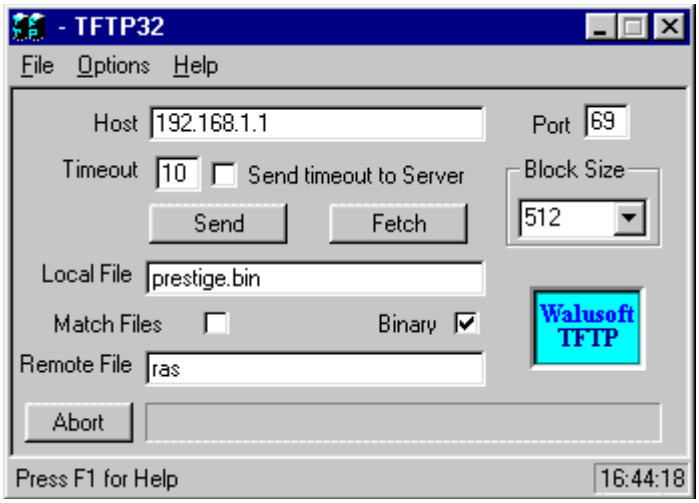
Step 2: Type the CI command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI)**

Step 3: Run the TFTP client software

Step 4: Enter the IP address of the P-793H v2

Step 5:To upload the firmware, please save the remote file as **'ras'** to P-793H v2. After the transfer is complete, the P-793H v2 will program the upgraded firmware into FLASH ROM and reboot itself.

An example:



The 192.168.1.1 is the IP address of the P-793H v2. The local file is the source file of the ZyNOS firmware that is available in your hard disk. The remote file is the file name that will be saved in P-793H v2. Check the port number 69 and 512-Octet blocks for TFTP. Check **'Binary'** mode for file transferring.

(2) Using TFTP to upload/download SMT configurations via LAN

Step 1: TELNET to your P-793H v2 first before running the TFTP software

Step 2: Type the command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI).**

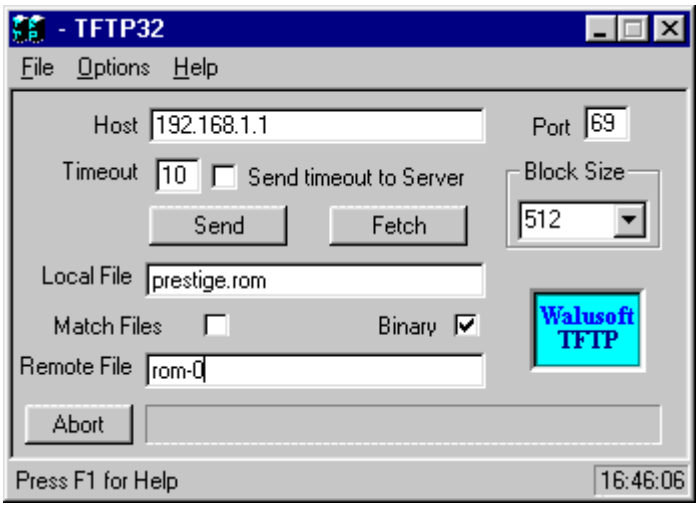
Step 3: Run the TFTP client software

Step 4: To download the P-793H v2 configuration, please get the remote file **'rom-0'** from the P-793H v2.

All contents copyright © 2010 ZyXEL Communications Corporation.

Step 5: To upload the P-793H v2configuration, please save the remote file as **'rom-0'** in the P-793H v2.

An example:



- The 192.168.1.1 is the IP address of the P-793H v2.
- The local file is the source file of your configuration file that is available in your hard disk.
- The remote file is the file name that will be saved in P-793H v2.
- Check the port number 69 and 512-Octet blocks for TFTP.
- Check 'Binary' mode for file transfering.

Using TFTP command on Windows NT

Step 1: TELNET to your P-793H v2 first before using TFTP command
Step 2: Type the CI command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI).**
Step 3: Download ZyNOS via LAN : **c:\tftp -i [P-793H v2IP] get ras [localfile]**
Step 4: Upload P-793H v2 configurations via LAN: **c:\tftp -i [P-793H v2 IP] put [localfile]**

rom-0

Step 5: Download P-793H v2 configurations via LAN: **c:\tftp -i [P-793H v2 IP] get rom-0**

[localfile]

Using TFTP command on UNIX

Before you begin:

1. TELNET to your P-793H v2 first before using TFTP command

All contents copyright © 2010 ZyXEL Communications Corporation.

2. Type the CI command 'sys stdio 0' to disable console idle timeout in **Command Line Interface (CLI)**

Example:

```
[cppwu@faelinux cppwu]$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Password: ****
ras> sys stdio 0
(Open a new window)
[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 get rom-0 [local-rom] <- change to binary mode

<- download configurations

[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 put [local-rom] rom-0 <- upload configurations

[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 get ras [local-ras ] <- download firmware

[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 put [local-ras] ras <- upload firmware
```

3. Using FTP to Upload the Firmware and Configuration Files

In addition to upload the firmware and configuration file via the console port and TFTP client, you can also upload the firmware and configuration files to the P-793H v2 using FTP.

To use this feature, your workstation must have a FTP client software. See the example shown below.

- **Using FTP client software**

Note: The remote file name for the firmware is **'ras'** and the configuration file is **'rom-0'**.

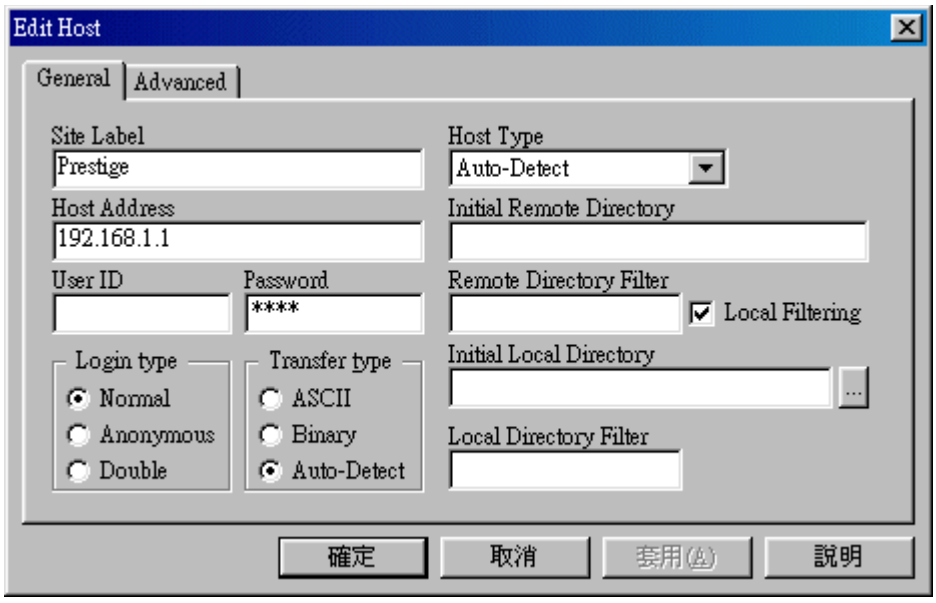
Step 1	Use FTP client from your workstation to connect to the P-793H v2 by entering the IP address of the P-793H v2.
Step2	Press **'Enter'** key to ignore the username, because the P-793H v2 doe not check the username.
Step 3	Enter the **CLI** password as the FTP login password, the default is **'admin'**.
Step 4	Enter command **'bin'** to set the transfer type to binary.

All contents copyright © 2010 ZyXEL Communications Corporation.

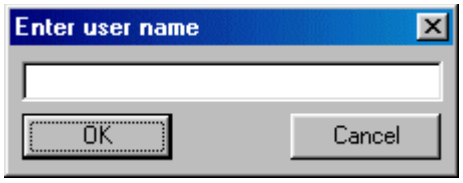
Step 5 Use **'put'** command to transfer the file to the P-793H v2.

Example:

Step 1: Connect to the P-793H v2 by entering the P-793H v2's IP and Administrator password in the FTP software. Set the transfer type to **'Auto-Detect'** or **'Binary'**.



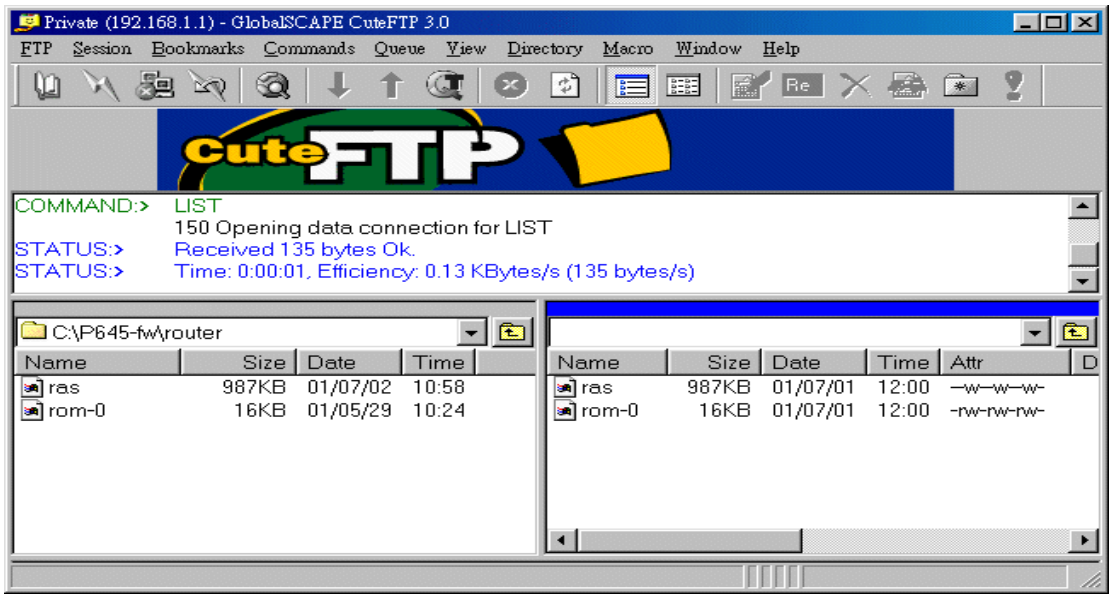
Step 2: Press **'OK'** to ignore the 'Username' prompt.



Step 3: To upload the firmware file, we transfer the local **'ras'** file to overwrite the remote **'ras'** file.
To upload the configuration file, we transfer the local **'rom-0'** to overwrite

All contents copyright © 2010 ZyXEL Communications Corporation.

the remote **'rom-0'** file.


Private (192.168.1.1) - GlobalSCAPE CuteFTP 3.0
FTP Session Bookmarks Commands Queue View Directory Macro Window Help
CuteFTP
COMMAND:> LIST
150 Opening data connection for LIST
STATUS:> Received 135 bytes Ok.
STATUS:> Time: 0:00:01, Efficiency: 0.13 KBytes/s (135 bytes/s)
C:\P645-fw\router
Name Size Date Time
ras 987KB 01/07/02 10:58
rom-0 16KB 01/05/29 10:24
Name Size Date Time Attr
ras 987KB 01/07/01 12:00 -w--w--w-
rom-0 16KB 01/07/01 12:00 -rw-rw-rw-

Step 4: The P-793H v2 reboots automatically after the uploading is finished. Please do not power off the router at this moment.

All contents copyright © 2010 ZyXEL Communications Corporation.

CI Command Reference

Command Syntax and General User Interface

CI has the following command syntax:

command <*iface* | *device* > **subcommand** [*param*]
command subcommand [*param*]
command ? | help
command subcommand ? | help

General user interface:

1.	**?**	Shows the following commands and all major (sub)commands
2.	**exit**	Exit Subcommand

To get the latest CI Command list

The latest CI Command list is available in release note of every ZyXEL firmware release. Please goto ZyXEL public WEB site http://www.zyxel.com/support/download_index.php to download firmware package (*.zip), you should unzip the package to get the release note in PDF format.

All contents copyright © 2010 ZyXEL Communications Corporation.

Reference

1. PPP Numbers

POINT-TO-POINT PROTOCOL FIELD ASSIGNMENTS

PPP DLL PROTOCOL NUMBERS

The Point-to-Point Protocol (PPP) Data Link Layer [146,147,175] contains a 16 bit Protocol field to identify the encapsulated protocol. The Protocol field is consistent with the ISO 3309 (HDLC) extension mechanism for Address fields. All Protocols MUST be assigned such that the least significant bit of the most significant octet equals "0", and the least significant bit of the least significant octet equals "1".

- **Network Layer Numbers**

Value (in hex)	Protocol Name
0001	Padding Protocol
0003 to 001f	reserved (transparency inefficient)
0021	Internet Protocol version 4
0023	OSI Network Layer
0025	Xerox NS IDP
0027	DECnet Phase IV
0029	AppleTalk
002b	Novell IPX
002d	Van Jacobson Compressed TCP/IP
002f	Van Jacobson Uncompressed TCP/IP
0031	Bridging PDU
0033	Stream Protocol (ST-II)
0035	Banyan Vines
0037	reserved (until 1993)
0039	AppleTalk EDDP
003b	AppleTalk SmartBuffered
003d	Multi-Link [RFC1717]
003f	NETBIOS Framing
0041	Cisco Systems
0043	Ascom Timeplex
0045	Fujitsu Link Backup and Load Balancing (LBLB)
0047	DCA Remote Lan
0049	Serial Data Transport Protocol (PPP-SDTP)
004b	SNA over 802.2

All contents copyright © 2010 ZyXEL Communications Corporation.

004d	SNA
004f	Pv6 Header Compression
0051	KNX Bridging Data [ianp]
0053	Encryption [Meyer]
0055	Individual Link Encryption [Meyer]
0057	Internet Protocol version 6 [Hinden]
006f	Stampede Bridging
0071	Reserved [Fox]
0073	MP+ Protocol [Smith]
007d	reserved (Control Escape) [RFC1661]
007f	reserved (compression inefficient) [RFC1662]
0081	Reserved Until 20-Oct-2000 [IANA]
0083	Reserved Until 20-Oct-2000 [IANA]
00c1	NTCITS IPI [Ungar]
00cf	reserved (PPP NLPID)
00fb	single link compression in multilink [RFC1962]
00fd	compressed datagram [RFC1962]
00ff	reserved (compression inefficient)

02xx-1exx	(compression inefficient)
0201	802.1d Hello Packets
0203	IBM Source Routing BPDU
0205	DEC LANBridge100 Spanning Tree
0207	Cisco Discovery Protocol [Sastry]
0209	Netcs Twin Routing [Korfmacher]
0231	Luxcom
0233	Sigma Network Systems
0235	Apple Client Server Protocol [Ridenour]
0281	Tag Switching - Unicast [Davie]
0283	Tag Switching - Multicast [Davie]
4001	Cray Communications Control Protocol [Stage]
4003	CDPD Mobile Network Registration Protocol [Quick]
4021	Stacker LZS [Simpson]
4023	RefTek Protocol [Banfill]

- **NCP Layer Number**

8001-801f	Not Used - reserved [RFC1661]
8021	Internet Protocol Control Protocol
8023	OSI Network Layer Control Protocol
8025	Xerox NS IDP Control Protocol
8027	DECnet Phase IV Control Protocol
8029	Appletalk Control Protocol

All contents copyright © 2010 ZyXEL Communications Corporation.

802b	Novell IPX Control Protocol
802d	reserved
802f	reserved
8031	Bridging NCP
8033	Stream Protocol Control Protocol
8035	Banyan Vines Control Protocol
8037	reserved till 1993
8039	reserved
803b	reserved
803d	Multi-Link Control Protocol
803f	NETBIOS Framing Control Protocol
8041	Cisco Systems Control Protocol
8043	Ascom Timeplex
8045	Fujitsu LBLB Control Protocol
8047	DCA Remote Lan Network Control Protocol (RLNCP)
8049	Serial Data Control Protocol (PPP-SDCP)
804b	SNA over 802.2 Control Protocol
804d	SNA Control Protocol
804f	IP6 Header Compression Control Protocol
8051	KNX Bridging Control Protocol [ianp]
8053	Encryption Control Protocol [Meyer]
8055	Individual Link Encryption Control Protocol [Meyer]
8057	IPv6 Control Protovol [Hinden]
806f	Stampede Bridging Control Protocol
8073	MP+ Control Protocol [Smith]
8071	Reserved [Fox]
807d	Not Used - reserved [RFC1661]
8081	Reserved Until 20-Oct-2000 [IANA]
8083	Reserved Until 20-Oct-2000 [IANA]
80c1	NTCITS IPI Control Protocol [Ungar]
80cf	Not Used - reserved [RFC1661]
80fb	single link compression in multilink control [RFC1962]
80fd	Compression Control Protocol [RFC1962]
80ff	Not Used - reserved [RFC1661]
8207	Cisco Discovery Protocol Control [Sastry]
8209	Netcs Twin Routing [Korfmacher]
8235	Apple Client Server Protocol Control [Ridenour]
8281	Tag Switching - Unicast [Davie]
8283	Tag Switching - Multicast [Davie]

- **LCP Layer Numbers**

All contents copyright © 2010 ZyXEL Communications Corporation.

c021	Link Control Protocol
c023	Password Authentication Protocol
c025	Link Quality Report
c027	Shiva Password Authentication Protocol
c029	CallBack Control Protocol (CBCP)
c02b	BACP Bandwidth Allocation Control Protocol [RFC2125]
c02d	BAP [RFC2125]
c081	Container Control Protocol [KEN]
c223	Challenge Handshake Authentication Protocol
c225	RSA Authentication Protocol [Narayana]
c227	Extensible Authentication Protocol [RFC2284]
c229	Mitsubishi Security Info Exch Ptcl (SIEP) [Seno]
c26f	Stampede Bridging Authorization Protocol
c281	Proprietary Authentication Protocol [KEN]
c283	Proprietary Authentication Protocol [Tackabury]
c481	Proprietary Node ID Authentication Protocol [KEN]

It is recommended that values in the "02xx" to "1exx" and "xx01" to "xx1f" ranges not be assigned, as they are compression inefficient. Protocol field values in the "0xxx" to "3xxx" range identify the network-layer protocol of specific datagrams, and values in the "8xxx" to "bxxx" range identify datagrams belonging to the associated Network Control Protocol (NCP), if any. Protocol field values in the "4xxx" to "7xxx" range are used for protocols with low volume traffic which have no associated NCP. Protocol field values in the "cxxx" to "exxx" range identify datagrams as Control Protocols (such as LCP).

PPP LCP AND IPCP CODES

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP), the Compression Control Protocol (CCP), Internet Protocol Control Protocol (IPCP), and other control protocols, contain an 8 bit Code field which identifies the type of packet. These Codes are assigned as follows:

Code	Packet Type
0	Vendor Specific [RFC2153]
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack

All contents copyright © 2010 ZyXEL Communications Corporation.

7 Code-Reject
8 * Protocol-Reject
9 * Echo-Request
10 * Echo-Reply
11 * Discard-Request
12 * Identification
13 * Time-Remaining
14 + Reset-Request [RFC1962]
15 + Reset-Reply [RFC1962]

* LCP Only
+ CCP Only

PPP LCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) specifies a number of Configuration Options which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
0	Vendor Specific [RFC2153]
1	Maximum-Receive-Unit
2	Async-Control-Character-Map
3	Authentication-Protocol
4	Quality-Protocol
5	Magic-Number
6	DEPRECATED (Quality-Protocol)
7	Protocol-Field-Compression
8	Address-and-Control-Field-Compression
9	FCS-Alternatives [RFC1570]
10	Self-Describing-Pad [RFC1570]
11	Numbered-Mode [RFC1663]
12	DEPRECATED (Multi-Link-Procedure)
13	Callback [RFC1570]
14	DEPRECATED (Connect-Time)
15	DEPRECATED (Compound-Frames)
16	DEPRECATED (Nominal-Data-Encapsulation)
17	Multilink-MRRU [RFC1717]
18	Multilink-Short-Sequence-Number-Header [RFC1717]
19	Multilink-Endpoint-Discriminator [RFC1717]
20	Proprietary [KEN]

All contents copyright © 2010 ZyXEL Communications Corporation.

21 DCE-Identifier [SCHNEIDER]
22 Multi-Link-Plus-Procedure [Smith]
23 Link Discriminator for BACP [RFC2125]
24 LCP-Authentication-Option [Culbert]
25 Consistent Overhead Byte Stuffing (COBS) [Carlson]
26 Prefix elision [Bormann]
27 Multilink header format [Bormann]

- IPV6CP CONFIGURATION OPTIONS

IPV6CP Configuration Options allow negotiation of desirable IPv6 parameters. IPV6CP uses the same Configuration Option format defined for LCP, with a separate set of Options. If a Configuration Option is not included in a Configure-Request packet, the default value for that Configuration Option is assumed.

1 Interface-Token [RFC2023]
2 IPv6-Compression-Protocol [RFC2023]

- PPP ECP CONFIGURATION OPTION TYPES

A one octet field is used in the Encryption Control Protocol (ECP) to indicate the configuration option type [RFC1968].

ECP Option	Configuration Type
0	OUI [RFC1968]
1	Deprecated (DESE) [Fox]
2	DESE [Kummert]
3	DESE-bis [Fox]
4-255	Unassigned

PPP CCP CONFIGURATION OPTION TYPES

A one octet field is used in the Compression Control Protocol (CCP) to indicate the configuration option type [RFC1962].

CCP Option	Configuration Type
0	OUI [RFC1962]
1	Predictor type 1 [RFC1962]
2	Rredictor type 2 [RFC1962]

All contents copyright © 2010 ZyXEL Communications Corporation.

3	Puddle Jumper [RFC1962]
4-15	unassigned
16	Hewlett-Packard PPC [RFC1962]
17	Stac Electronics LZS [RFC1974]
18	Microsoft PPC [RFC2118]
19	Gandalf FZA [RFC1962]
20	V.42bis compression [RFC1962]
21	BSD Compress [RFC1977]
22	unassigned
23	LZS-DCP [RFC1967]
24	MVRCA (Magnalink) [RFC1975]
25	DCE [RFC1976]
26	Deflate [RFC1979]
27-254	unassigned
255	Reserved [RFC1962]

The unassigned values 4-15 are intended to be assigned to other freely available compression algorithms that have no license fees.

- PPP SDCP CONFIGURATION OPTIONS

A one octet field is used in the Compression Control Protocol (CCP) PPP Serial Data Transport Protocol (SDTP) to indicate the option type [RFC1963].

SDCP Option	Configuration Element
1	Packet-Format [RFC1963]
2	Header-Type [RFC1963]
3	Length-Field-Present [RFC1963]
4	Multi-Port [RFC1963]
5	Transport-Mode [RFC1963]
6	Maximum-Frame-Size [RFC1963]
7	Allow-Odd-Frames [RFC1963]
8	FCS-Type [RFC1963]
9	Flow-Expiration-Time [RFC1963]

Note that Option Types 5-8 are specific to a single port and require port numbers in their format. Option Types 6-8 are specific to the HDLC-Synchronous Transport-Mode.

- **PPP AUTHENTICATION ALGORITHMS**

All contents copyright © 2010 ZyXEL Communications Corporation.

A one octet field is used in the Challenge-Handshake Authentication Protocol (CHAP) to indicate which algorithm is in use [RFC1994].

Number	Name
0	Reserved [RFC1994]
1	Reserved [RFC1994]
2	Reserved [RFC1994]
3	Reserved [RFC1994]
4	Reserved [RFC1994]
5	CHAP with MD5 [RFC1994]
128	MS-CHAP [Crocker]
PPP	LCP FCS-ALTERNATIVES

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) FCS-Alternatives Configuration Option contains an 8-bit Options field which identifies the FCS used. These are assigned as follows:

Bit	FCS
1	Null FCS
2	CCITT 16-Bit FCS
4	CCITT 32-bit FCS

- PPP MULTILINK ENDPOINT DISCRIMINATOR CLASS

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) Multilink Endpoint Discriminator Option includes a Class field which identifies the address class, These are assigned as follows:

Class	Description
0	Null Class [RFC1717]
1	Locally Assigned [RFC1717]
2	Internet Protocol (IPv4) [RFC1717]
3	IEEE 802.1 global MAC address [RFC1717]
4	PPP Magic Number Block [RFC1717]
5	Public Switched Network Director Number [RFC1717]

- PPP LCP CALLBACK OPERATION FIELDS

All contents copyright © 2010 ZyXEL Communications Corporation.

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) Callback Configuration Option contains an 8-bit Operations field which identifies the format of the Message. These are assigned as follows:

Operation	Description
0	Location determined by user authentication.
1	Dialing string.
2	Location identifier.
3	E.164 number.
4	X.500 distinguished name.
5	unassigned
6	Location is determined during CBCP negotiation.

- **PPP IPCP CONFIGURATION OPTION TYPES**

The Point-to-Point Protocol (PPP) Internet Protocol Control Protocol (IPCP) specifies a number of Configuration Options which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	IP-Addresses (deprecated) [RFC1332]
2	IP-Compression-Protocol [RFC1332]
3	IP-Address [RFC1332]
4	Mobile-IPv4 [RFC2290]
129	Primary DNS Server Address [RFC1877]
130	Primary NBNS Server Address [RFC1877]
131	Secondary DNS Server Address [RFC1877]
132	Secondary NBNS Server Address [RFC1877]

- PPP ATCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Apple Talk Control Protocol (ATCP) specifies a number of Configuration Options [RFC-1378] which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	AppleTalk-Address
2	Routing-Protocol
3	Suppress-Broadcasts

All contents copyright © 2010 ZyXEL Communications Corporation.

4	AT-Compression-Protocol
5	Reserved
6	Server-information
7	Zone-information
8	Default-Router-Address

- PPP OSINLCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) OSI Network Layer Control Protocol (OSINLCP) specifies a number of Configuration Options [RFC1377] which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	Align-NPDU

- PPP BANYAN VINES CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Banyan Vines Control Protocol (BVCP) specifies a number of Configuration Options [RFC1763] which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	BV-NS-RTP-Link-Type
2	BV-FRP
3	BV-RTP
4	BV-Suppress-Broadcast

- PPP BRIDGING CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP) specifies a number of Configuration Options which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	Bridge-Identification
2	Line-Identification
3	MAC-Support
4	Tinygram-Compression
5	LAN-Identification

All contents copyright © 2010 ZyXEL Communications Corporation.

6 MAC-Address
7 Spanning-Tree-Protocol

- PPP BRIDGING MAC TYPES

The Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP) contains an 8 bit MAC Type field which identifies the MAC encapsulated. These Types are assigned as follows:

Type	MAC
0	Reserved
1	IEEE 802.3/Ethernet with cannonical addresses
2	IEEE 802.4 with cannonical addresses
3	IEEE 802.5 with non-cannonical addresses
4	FDDI with non-cannonical addresses
5-10	reserved
11	IEEE 802.5 with cannonical addresses
12	FDDI with cannonical addresses

- PPP BRIDGING SPANNING TREE

The Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP) Spanning Tree Configuration Option contains an 8-bit Protocol field which identifies the spanning tree used. These are assigned as follows:

Protocol	Spanning Tree
0	Null - no spanning tree protocol supported
1	IEEE 802.1D spanning tree protocol
2	IEEE 802.1G extended spanning tree protocol
3	IBM source route spanning tree protocol
4	DEC LANbridge 100 spanning tree protocol

- PPP INTERNETWORK PACKET EXCHANGE CONTROL PROTOCOL (IPXCP)

IPXCP CONFIGURATION OPTIONS

Option	Description Reference
1	IPX-Network-Number [RFC1552]

All contents copyright © 2010 ZyXEL Communications Corporation.

2 IPX-Node-Number [RFC1552]
3 IPX-Compression-Protocol [RFC1552]
4 IPX-Routing-Protocol [RFC1552]
5 IPX-Router-Name [RFC1552]
6 IPX-Configuration-Complete [RFC1552]

- IPX COMPRESSION PROTOCOL VALUES

Value	Protocol Reference
2	Telebit Compressed IPX [Fox]
235	Shiva Compressed NCP/IPX [Fox]

- IPX-ROUTING-PROTOCOL OPTIONS

Value	Protocol Reference
0	No routing protocol required [RFC1552]
1	RESERVED [RFC1552]
2	Novell RIP/SAP required [RFC1552]
4	Novell NLSP required [RFC1552]
5	Novell Demand RIP required [RFC1582]
6	Novell Demand SAP required [RFC1582]
7	Novell Triggered RIP required [Edmonstone]
8	Novell Triggered SAP required [Edmonstone]

- NBFCP Configuration Options

NBFCP Configuration Options [RFC 2097] allow modifications to the standard characteristics of the network-layer protocol to be negotiated. If a Configuration Option is not included in a Configure-Request packet, the default value for that Configuration Option is assumed.

NBFCP uses the same Configuration Option format defined for LCP, with a separate set of Options.
Current values are assigned as follows:

1 Name-Projection
2 Peer-Information
3 Multicast-Filtering
4 IEEE-MAC-Address-Required

All contents copyright © 2010 ZyXEL Communications Corporation.

- PPP EAP REQUEST/RESPONSE TYPES

A one octet field is used in the Extensible Authentication Protocol (EAP) to indicate the function and structure of EAP Request and Response packets [RFC2284].

Type	Description
1	Identity [RFC2284]
2	Notification [RFC2284]
3	Nak (Response only) [RFC2284]
4	MD5-Challenge [RFC2284]
5	One Time Password (OTP) [RFC2289]
6	Generic Token Card [RFC2284]
7	
8	
9	RSA Public Key Authentication [Whelan]
10	DSS Unilateral [Nace]
11	KEA [Nace]
12	KEA-VALIDATE [Nace]
13	EAP-TLS [Adoba]
14	Defender Token (AXENT) [Rosselli]

- PPP VENDOR SPECIFIC OUI OPTIONS

There are some provisions in some PPP message formats for vendor specific options to be identified by the Organisationally Unique Identifier (OUI), namely the first three octets of a Vendor's Ethernet address assigned by IEEE 802 [RFC1968. RFC2153]. These are listed in the "ethernet-numbers" file (see http://www.iana.org/in-notes/iana/assignments/ethernet-numbers).

2. Port Numbers

The following list contains port numbers for well-known services as defined by RFC 1060 (Assigned Numbers).

Format:

<service name> <port number>/<protocol> [aliases...] [#<comment>]

echo 7/tcp
echo 7/udp

All contents copyright © 2010 ZyXEL Communications Corporation.

```
discard         9/tcp     sink null
discard         9/udp     sink null
systat          11/tcp
systat          11/tcp    users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp    quote
qotd            17/udp    quote
chargen         19/tcp    ttytst source
chargen         19/udp    ttytst source
ftp-data        20/tcp
ftp             21/tcp
telnet          23/tcp
smtp            25/tcp    mail
time            37/tcp    timserver
time            37/udp    timserver
rlp             39/udp    resource        # resource location
name            42/tcp    nameserver
name            42/udp    nameserver
whois           43/tcp    nicname         # usually to sri-nic
domain          53/tcp    nameserve       # name-domain server
domain          53/udp    nameserver
nameserver      53/tcp    domain          # name-domain server
nameserver      53/udp    domain
mtp             57/tcp                    # deprecated
bootp           67/udp                    # boot program server
tftp            69/udp
rje             77/tcp    netrjs
finger          79/tcp
link            87/tcp    ttylink
supdup          95/tcp
hostnames       101/tcp   hostname        # usually from sri-nic
iso-tsap        102/tcp
dictionary      103/tcp   webster
x400            103/tcp                   # ISO Mail
x400-snd        104/tcp
csnet-ns        105/tcp
pop             109/tcp   postoffice
pop2            109/tcp                   # Post Office
pop3            110/tcp   postoffice
portmap         111/tcp
portmap         111/udp
sunrpc          111/tcp
```


All contents copyright © 2010 ZyXEL Communications Corporation.

```
sunrpc          111/udp
auth            113/tcp      authenticatior
sftp            115/tcp
path            117/tcp
uucp-path       117/tcp
nntp            119/tcp      usenet       # Network News Transfer
ntp             123/udp      ntpd ntp     # network time protocol
nbname          137/udp
nbdatagram      138/udp
nbsession       139/tcp
NeWS            144/tcp    news
sgmp            153/udp     sgmp
tcprepo         158/tcp     repository    # PCMAIL
snmp            161/udp     snmp
snmp-trap       162/udp   snmp
print-srv       170/tcp                   # network PostScript
vmnet           175/tcp
load            315/udp
vmnet0
400/tcp sytek
                500/udp
biff            512/udp  comsat
exec            512/tcp
login           513/tcp
who             513/udp    whod
shell           514/tcp cmd           # no passwords used
syslog          514/udp
printer         515/tcp    spooler       # line printer spooler
talk            517/udp
ntalk           518/udp
efs             520/tcp               # for LucasFilm
route           520/udp    router routed
timed           525/udp     timeserver
tempo           526/tcp     newdate
courier         530/tcp     rpc
conference      531/tcp     chat
rvd-control     531/udp     MIT disk
netnews         532/tcp     readnews
netwall         533/udp               # -for emergency broadcasts
uucp            540/tcp    uucpd         # uucp daemon
klogin          543/tcp               # Kerberos authenticated rlogin
kshell          544/tcp  cmd          # and remote shell
new-rwho        550/udp     new-who       # experimental
remotefs        556/tcp    rfs_server rfs# Brunhoff remote filesystem
rmonitor        560/udp     rmonitord     # experimental
```


All contents copyright © 2010 ZyXEL Communications Corporation.

```
monitor         561/udp                 # experimental
garcon          600/tcp
maitrd          601/tcp
busboy          602/tcp
acctmaster      700/udp
acctslave       701/udp
acct            702/udp
acctlogin       703/udp
acctprinter     704/udp
elcsd           704/udp                 # errlog
acctinfo        705/udp
acctslave2      706/udp
acctdisk        707/udp
kerberos        750/tcp   kdc           # Kerberos authentication--tcp
kerberos        750/udp   kdc           # Kerberos authentication--udp
kerberos_master 751/tcp                 # Kerberos authentication
kerberos_master 751/udp                 # Kerberos authentication
passwd_server   752/udp                 # Kerberos passwd server
userreg_server  753/udp                 # Kerberos userreg server
krb_prop        754/tcp                 # Kerberos slave propagation
erlogin         888/tcp                 # Login and environment passing
kpop            1109/tcp                # Pop with Kerberos
phone           1167/udp
ingreslock      1524/tcp
maze            1666/udp
nfs             2049/udp                # sun nfs
knetd           2053/tcp                # Kerberos de-multiplexor
eklogin         2105/tcp                # Kerberos encrypted rlogin
rmt             5555/tcp    rmtd
mtb             5556/tcp    mtbd        # mtb backup
man             9535/tcp                # remote man server
w               9536/tcp
mantst          9537/tcp                # remote man server, testing
bnews           10000/tcp
rscs0           10000/udp
queue           10001/tcp
rscs1           10001/udp
poker           10002/tcp
rscs2           10002/udp
gateway         10003/tcp
rscs3           10003/udp
remp            10004/tcp
rscs4           10004/udp
rscs5           10005/udp
```


All contents copyright © 2010 ZyXEL Communications Corporation.

rscs6	10006/udp
rscs7	10007/udp
rscs8	10008/udp
rscs9	10009/udp
rscsa	10010/udp
rscsb	10011/udp
qmaster	10012/tcp
qmaster	10012/udp

3. Protocol Numbers

In the Internet Protocol version 4 (IPv4) [RFC791] there is a field, called "Protocol", to identify the next level protocol. This is an 8 bit field. In Internet Protocol version 6 (IPv6) [RFC1883] this field is called the "Next Header" field.

Assigned Internet Protocol Numbers

Decimal	Keyword	Protocol	References
0	HOPOPT	IPv6 Hop-by-Hop Option	[RFC1883]
1	ICMP	Internet Control Message	[RFC792]
2	IGMP	Internet Group Management	[RFC1112]
3	GGP	Gateway-to-Gateway	[RFC823]
4	IP	IP in IP	[RFC2003]
5	ST	Stream	[RFC1190,IEN119]
6	TCP	Transmission Control	[RFC793]
7	CBT	CBT	[Ballardie]
8	EGP	Exterior Gateway	[RFC888,DLM1]
9	IGP	any private interior gateway (used Cisco for their IGRP)	[IANA]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]
11	NVP-II	Network Protocol	[RFC741,SC3]
12	PUP	PUP	[PUP,XEROX]
13	ARGUS	ARGUS	[RWS4]
14	EMCON	EMCON	[BN7]
15	XNET	Cross Debugger	[IEN158,JFH2]
16	CHAOS	Chaos	[NC3]
17	UDP	User Datagram	[RFC768,JBP]
18	MUX	Multiplexing	[IEN90,JBP]
19	DCN-MEAS	DCN Measurement Subsystems	[DLM1]
20	HMP	Host Monitoring	[RFC869,RH6]
21	PRM	Packet Radio Measurement	[ZSU]

All contents copyright © 2010 ZyXEL Communications Corporation.

22	XNS-IDP	XEROX NS IDP	[ETHERNET,XEROX]
23	TRUNK-1	Trunk-1	[BWB6]
24	TRUNK-2	Trunk-2	[BWB6]
25	LEAF-1	Leaf-1	[BWB6]
26	LEAF-2	Leaf-2	[BWB6]
27	RDP	Reliable Protocol	[RFC908,RH6]
28	IRTP	Internet Reliable Transaction	[RFC938,TXM]
29	ISO-TP4	ISO Transport Protocol Class 4	[RFC905,RC77]
30	NETBLT	Bulk Data Transfer Protocol	[RFC969,DDC1]
31	MFE-NSP	MFE Network Services Protocol	[MFENET,BCH2]
32	MERIT-INP	MERIT Internodal Protocol	[HWB]
33	SEP	Sequential Exchange Protocol	[JC120]
34	3PC	Third Party Connect Protocol	[SAF3]
35	IDPR	Inter-Domain Routing Protocol	[MXS1]
36	XTP	XTP	[GXC]
37	DDP	Datagram Protocol	[WXC]
38	IDPR-CMTP	IDPR Control Message Transport Proto	[MXS1]
39	TP++	TP++ Transport Protocol	[DXF]
40	IL	IL Transport Protocol	[Presotto]
41	IPv6	Ipv6	[Deering]
42	SDRP	Source Routing Protocol	[DXE1]
43	IPv6-Route	Routing Header for IPv6	[Deering]
44	IPv6-Frag	Fragment Header for IPv6	[Deering]
45	IDRP	Inter-Domain Routing Protocol	[Sue Hares]
46	RSVP	Reservation Protocol	[Bob Braden]
47	GRE	General Routing Encapsulation	[Tony Li]
48	MHRP	Mobile Routing Protocol	[David
49	BNA	BNA	[Gary
50	ESP	Encap Payload for IPv6	[RFC1827]
51	AH	Authentication Header for IPv6	[RFC1826]
52	I-NLSP	Integrated Layer Security TUBA	[GLENN]
53	SWIPE	Net tion	[JI6]
54	NARP	NBMA Address esolution Protocol	[RFC1735]
55	MOBILE	R	[Perkins]
56	TLSP	Transport Layer Security Protocol using Kryptonet key management	[Oberg]
57	SKIP	SKIP	[Markson]
58	IPv6-ICMP	ICMP IPv6	[RFC1883]
59	IPv6-NoNxt	No Next Header for IPv6	[RFC1883]
60	IPv6-Opts	Destination Options for IPv6	[RFC1883]
61		any host internal protocol	[IANA]
62	CFTP	CFTP	[CFTP,HCF2]
63		any local network	[IANA]
64	SAT-EXPAK	SATNET and Backroom EXPAK	[SHB]

All contents copyright © 2010 ZyXEL Communications Corporation.

65	KRYPTOLAN	Kryptolan	[PXL1]
66	RVD	MIT Remote Disk Protocol	[MBG]
67	IPPC	Internet Pluribus Packet Core	[SHB]
68		any distributed file system	[IANA]
69	SAT-MON	SATNET Monitoring	[SHB]
70	VISA	VISA Protocol	[GXT1]
71	IPCV	Interne Packet Core Utility	[SHB]
72	CPNX	Computer Protocol Network Executive	[DXM2]
73	CPHB	Computer Protocol Heart Beat	[DXM2]
74	WSN	Wang Span Network	[VXD]
75	PVP	Packet Video Protocol	[SC3]
76	BR-SAT-MON	Backroom SATNET Monitoring	[SHB]
77	SUN-ND	SUN ND PROTOCOL-Temporary	[WM3]
78	WB-MON	WIDEBAND Monitoring	[SHB]
79	WB-EXPAK	WIDEBAND EXPAK	[SHB]
80	ISO-IP	ISO Internet Protocol	[MTR]
81	VMTP	VMTP	[DRC3]
82	SECURE-VMTP	SECURE-VMTP	[DRC3]
83	VINES	VINES	[BXH]
84	TTP	TTP	[JXS]
85	NSFNET-IGP	NSFNET-IGP	[HWB]
86	DGP	Dissimilar Protocol	[DGP,ML109]
87	TCF	TCF	[GAL5]
88	EIGRP	EIGRP	[CISCO,GXS]
89	OSPFIGP	OSPFIGP	[RFC1583,JTM4]
90	Sprite-RPC	Sprite RPC Protocol	[SPRITE,BXW]
91	LARP	Locus Address Resolution Protocol	[BXH]
92	MTP	Multicast Transport Protocol	[SXA]
93	AX.25	AX.25 Frames	[BK29]
94	IPIP	IP-within-IP Encapsulation Protocol	[JI6]
95	MICP	Mobile Internetworking Control Pro.	[JI6]
96	SCC-SP	Semaphore Communications Sec. Pro.	[HXH]
97	ETHERIP	Ethernet-within-IP Encapsulation	[RXH1]
98	ENCAP	Encapsulation Header	[RFC1241,RXB3]
99		any private encryption scheme	[IANA]
100	GMTP	GMTP	[RXB5]
101	IFMP	Ipsilon Management Protocol	[Hinden]
102	PNNI	PNNI over IP	[Callon]
103	PIM	Protocol Multicast	[Farinacci]
104	ARIS	ARIS	[Feldman]
105	SCPS	SCPS	[Durst]
106	QNX	QNX	[Hunter]
107	A/N	Active Networks	[Braden]
108	IPPCP	IP Payload Compression Protocol	[Doraswamy]

All contents copyright © 2010 ZyXEL Communications Corporation.

109	SNP	Sitara Networks Protocol	[Sridhar]
110	Compaq-Peer	Compaq Peer Protocol	[Volpe]
111	IPX-in-IP	IPX in IP	[Lee]
112	VRRP	Virtual Router Redundancy Protocol	[Hinden]
113	PGM	PGM Reliable Transport Protocol	[Speakman]
114		any 0-hop protocol	[IANA]
115	L2TP	Layer Two Tunneling Protocol	[Aboba]
116-254		Unassigned	[IANA]
255		Reserved	[IANA]

All contents copyright © 2010 ZyXEL Communications Corporation.